



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 18: Issue 1

Friday 5 April 1996

Contents

- [Sixth Computers, Freedom and Privacy](#)
[Shabbir J. Safdar](#)
- [A Wiretap Incident in New Orleans](#)
[Shabbir J. Safdar](#)
- [Computer Error Costs MCI \\$Millions](#)
[Scott Lucero](#)
- [Teen Accused of Hacking](#)
[David M Kennedy](#)
- [Only Americans can contact the AT&T operator](#)
[Tom Gardner](#)
- [Re: Wrong approach to Java security](#)
[Frank Stuart](#)
- [Re: Risks of rewritable BIOSes](#)
[Jeremy J Epstein](#)
- [Re: "This is not a bug" messages: MacsBug](#)
[David A. Lyons](#)
- [Re: The Queen's Speech](#)
[Allan Engelhardt](#)
- [Re: Notes on e-mail: Use of diaeresis](#)
[Dan Hicks](#)

[Daan Sandee](#)

● [On the meaning of "email"](#)

[Clive Feather](#)

● [Browser return e-mail addresses](#)

[Walter Roberson](#)

● [Info on RISKS \(comp.risks\)](#)

⚡ **Sixth Computers, Freedom and Privacy**

Shabbir J. Safdar <shabbir@vtw.org>

Thu, 04 Apr 1996 16:05:34 -0500

I attended last week's Sixth Computers, Freedom, and Privacy conference in Cambridge MA, where policy-makers, technical experts, and activists came together to hash out the intersection of the three elements of its title. CFP is an unusual place; the closest thing our community can get to "neutral ground" on many issues. This is best expressed by the fact that in the hallways of the hotel, it's not unusual to see those that supported and those that fought the Communications Decency Act hob-nobbing it up, trading friendly swipes about their take on the bill.

In addition, it's always an enjoyable thing to be able to meet an FBI agent in a neutral setting and ask them questions about their perspective on various issues.

CFP is still finding it's way, though, as the issues it covers evolve in and out of the mainstream. A few years ago the issues were hackers and search warrants for computers and bulletin boards. Now that seems to

have been replaced by encryption policy, wiretaps and how much of the First Amendment applies to the net.

CFP has survived well, and I continue to return every year I can. I return not only see the issues from new perspectives, but also to obtain the synergy that can only happen in a face-to-face encounter.

This isn't to say that CFP doesn't stumble occasionally. There were a few panels this year that fell into the CFP trap, where individuals came to express none-to-fresh perspectives on problems that have been beaten like the Lone Ranger's dead steed. Encryption is typically the cause of these.

On the other hand, however, CFP was successful in what is the most entertaining and enlightening approach to the encryption debate I've seen in the last two years. Centering around a mock law that required key escrow, the CFP program committee set up a "moot court" of five Federal judges (real ones, with black robes and everything) that heavily questioned attorneys that presented a cases for the government on one side, and plaintiffs challenging the law on the other.

The live questioning, and the exercise of having to put one's arguments into a legal framework was an experience that everyone enjoyed. This was clearly the most heavily attended panel of the conference.

The other interesting thing this year was the final panel of the conference, a reflection on the entire conference done by four science

fiction authors:

Bruce Sterling, Vernor Vinge, Pat Cadigan, and Tom Maddox. This was probably the most interesting way to reflect on the conference, and the writers seemed to form a sort of "collective conscience" for the rest of us.

Bruce Sterling, in particular, provided a dystopian view with such a forceful delivery that I, and many others, probably stumbled from the room unable to decide if we were happy we knew where we were going, or if we should run screaming in terror at society's impending train wreck.

It was somewhat appropriate that there was no time for questions after that panel. They would have simply detracted from the fact that the writers got the "last word".

It's a great role though, to have those who dream for us, our science fiction writers, act as our conscience. I hope the program committee lets them do it next year, and I look forward to meeting the next set of faces that I'll have met on the net over the next year.

-Shabbir J. Safdar * Online Representative * Voters Telecomm. Watch (VTW)

<http://www.vtw.org/> * Defending Your Rights In Cyberspace

[Note: This was a very lively meeting. I hope further reportage will

appear in RISKS. By the way, Shabbir, Matt Blaze, Bob Metcalfe and I were

honored with this year's EFF Pioneer Awards. Greatly appreciated! PGN]

⚡ A Wiretap Incident in New Orleans

Shabbir J. Safdar <shabbir@vtw.org>

Thu, 04 Apr 1996 16:05:34 -0500

[From VTW's BillWatch newsletter, an announcement-only list archived at

<http://www.vtw.org/billwatch/>]

-Shabbir J. Safdar * Online Representative * Voters Telecomm. Watch (VTW)

<http://www.vtw.org/> * Defending Your Rights In Cyberspace

A TRAGIC STORY ABOUT A WIRETAP by Shabbir J. Safdar, VTW Board (New York, NY)

This week most of VTW's staff attended the Computers, Freedom, and Privacy conference in Cambridge Massachusetts. I go to the conference every year to recharge my batteries, put names to faces, and enjoy the synergy that can only come with face-to-face dialogue.

This year the debate over encryption seemed focused on three panels, the only novel one being a panel which was a "moot court". Presided over by five real Federal judges, attorneys for plaintiffs and the government argued over the Constitutionality of a mock law that would require escrowing of encryption keys. Aside from this, the conference added no new material to the encryption debate.

One valuable experience happened on the way home, however. I picked up the New York Times and came across a story in the New York Times Magazine about

a corrupt New Orleans police chief, and how he reacted to a woman who filed a police brutality complaint against him.

The story goes this way: the FBI was wiretapping a number of New Orleans police officers who were allegedly guarding a 286 pound shipment of cocaine.

During that time the FBI overheard a conversation between the police chief and several other police officials that the FBI alleges was a murder plot.

The intended victim had previously filed a police brutality complaint against the chief.

Although the FBI had the conversation in hand, they were unable to decode the police chief's "street slang and police jargon" in time to prevent the murder. The woman who filed the complaint, a 32 year old mother of three, was shot while standing in front of her house.

It's easy to be angry about this incident. One could (and should) be angry with the murderers and their conspirators. However out of this comes two important observations on the encryption policy debate.

One, while wiretaps have probably been effective in other cases, they were not effective in this one. While we can grant law enforcement the benefit of the doubt in other cases, the existence of this one shows that a wiretap is not the "silver bullet" of law enforcement that we have been led to believe.

Another observation that can be made is that this parallels the key escrow debate very closely. No reasonable person is objecting to the

FBI's right

to conduct a wiretap. However what is being debated is the extent to which

individuals and law enforcement can go to accomplish their duties. The

Clinton Administration is striving for a world where everyone is forced to

speak in a form of encryption that is easily decoded by law enforcement.

The public and industry is striving for a world where they continue to have

private conversations.

The situational parallel to this would be if the Administration had pushed a

law that requires everyone to speak on the telephone in plain English,

without slang and without any double meanings. This is the equivalent of

key escrow.

However, would this have really saved the person so tragically killed above?

Unlikely. Individuals involved in criminal conspiracies will continue to

use whatever means at their disposal to obscure their activities from the

police. The corrupt police chief who allegedly ordered the murder would

have still used slang and code, regardless of any laws banning such use. He

was allegedly conspiring to commit a murder, why should he care?

Such laws will, however, affect law abiding citizen's attempts to gain

privacy. Law-abiding citizens that may be speaking to their doctors,

attorneys, loved-ones, or business partners will continue to be targets of

industrial espionage, private investigators, and, in a few cases, trusted

individuals abusing that trust.

This example from the New York Times Magazine (3/31/96, p.32) shows that while we can certainly give a little to law enforcement on their arguments about the effectiveness of wiretaps, they need to give a little in the other direction on the practicality of forcing people to speak in a law-enforcement-understandable code. Obviously, criminals don't care about such rules. Since that is the case, is it really worth handicapping all technology, and exposing individuals to privacy intrusions when such measures won't even be effective at attaining their stated goals?

⚡ Computer Error Costs MCI \$Millions

"lucero" <lucero@optec.army.mil>

Wed, 03 Apr 96 15:15:29 EST

In the **Washington Post** 29 March 1996, MCI reported that they will refund approximately \$40 million due to a computer error. A billing error was uncovered by an investigative reporter from local television station, WRIC in Richmond, VA. The reporters found that they were charged for 4 minutes after making a 2.5 minute call, leading to an in-depth investigation.

Scott Lucero

⚡ Teen Accused of Hacking

David M Kennedy <David_M_Kennedy@smtp.ord.usace.army.mil>

Thu, 04 Apr 1996 16:28:49 -0500

Courtesy of the Associated Press via CompuServe's Executive News Service:

AP 2 Apr 96 20:21 EST V0491

>> ST. LOUIS (AP) -- A St. Louis teen-ager arrested last week near Philadelphia on computer fraud charges is more than just a kid with a hobby -- and far more dangerous, federal authorities say. Christopher Schanot, 19, of High Ridge, Mo., is a computer genius who "hacked" his way into the computers of some of the nation's largest computers, causing security breaches that forced at least one company to spend thousands of dollars fixing.<<

o Authorities claim he's a member of the Internet Liberation Front (ILF).

o He claims to be able to take control of any computer he chooses to.

o He was taken to St. Louis Tuesday with a arraignment and bond hearing set for Thursday.

o His father was quoted: "If a parent can't monitor the child or if the parent doesn't understand how the Internet works, the computer's modem should be unplugged." The younger Schanot received his first computer at the age of 4 years. His father was quoted as instructing him to use only public access computer systems and, "He was an honor student, really he was all you could want in a child. It was such a shock to us when he disappeared."

- o He was an honors student at Vianney High School in suburban St. Louis.

Shortly after graduation last summer he went to Philadelphia to "lay low."

- o His father became concerned about him and contacted the authorities and turned over his PC to them.

>>In the computer, authorities found a message headed "Greetings from the Internet Liberation Front." The message was saved to his computer on Thanksgiving Day 1994, the day of a computerized "break-in" at NBC. The message said the group "has now declared war on any company suspected of contributing to the final demise of the Internet." "Big boys" in the telecommunication industry have turned the Internet "into another overflowing cesspool of greed," the message added. "We are capable of penetrating virtually any network linked to the Internet -- ANY network," the message said. <<

[DMK: Gee, that was in RISKS and any number of net-news reports back in 94.

The only reason it's not on my PC is I purged it to save disk space. Does that qualify me as a "purged" ILF member?]

- o His PC also had hundreds of passwords to corporate computer systems, including defense contractors and the computers of credit reporting agencies. The PC also had AT&T calling card numbers, and credit card numbers in it.

- o He was indicted on five counts (unspecified...18 USC 1029/1030?) last

month. Max slammer time = 30 years + US\$1.25E06 in fines.

o Victims: Southwestern Bell Telephone, BELLCORE, Sprint, and SRI.

o Time frame: Oct 24, 1994 to Apr 23, 1995

MAJ Dave Kennedy [CISSP]

✶ Only Americans can contact the AT&T operator

Tom Gardner <tgg@hplb.hpl.hp.com>

Tue, 02 Apr 1996 16:05:53 -0800

Tom Gardner
Filton Rd,
tgg@hpl.hp.com
6QZ, ENGLAND.

Hewlett Packard Laboratories,
Stoke Gifford, Bristol, Avon, BS12
Tel: +44 117 9799910 ext. 28192
Fax: +44 117 9228920

Subject: I Cannot Call The AT&T Operator

While in the US, I recently wanted to find out a number in England, and since I don't know the local directory enquiries number, I called the AT&T operator. After dialling "00" the "conversation" between me and the abuser interface (ABI) was:

ABI: "AT&T. To place a call, please dial the number now, or say 'operator' to be connected to an operator".

Me: "Operator"

ABI: "Sorry, your response was not understood. To place a call, please dial the number now, or say 'operator' to be connected to the operator".

Me: "Operator"

ABI: "Sorry, your response was not understood..."

Thus the abuser interface would only allow me to do the single thing that I didn't know how to do. After a few more abortive attempts I found that the necessary incantation involved pinching my nose and saying "er-per-eight-er".

The risk? That people with speech impediments, and ethnic minorities who do not speak with a "standard" US accent (i.e., the majority of the human race!) cannot be connected with an operator, and are thus unable to place telephone calls. The abuser interface would have been perfectly acceptable if there had been an additional escape clause such as "...or wait for 30 seconds to be connected to an operator".

On a separate but related issue, can anyone tell me whether the codecs in "digital" cellular phones are usable with non-Indo-European languages such as:

- languages where the pitch is extremely important but the "consonants" are relatively unimportant, e.g. (I believe) Mandarin Chinese
- the African "click" languages

[Tom, ``Standard US?'' Many North "Americans" have troubles. Regional dialects here are pretty severe. But certainly Cockney, Australian * ('Strine), and other variants of English are unlikely to be decoded.

I suppose we all need the language training that actors get. I am always astounded when I hear a Brit or Aussie actor known for wonderful BEnglish

or AusEnglish dialect speaking perfect AEnglish. Just a thought. PGN]

[* Slight spelling correction in archive copy to ward off pe-roo-sers.]

⚡ Re: Wrong approach to Java security (Palme, [RISKS-17.95](#))

Frank Stuart <fstuart@vetmed.auburn.edu>

Mon, 1 Apr 1996 19:57:37 -0600 (CST)

In [RISKS-17.95](#), Jacob Palme suggests that the reputation of "well-kept depositories" and PICS-like ratings can be used to guard against malicious Java code. A more useful idea along the same lines is to allow for code to carry a digital signature. A user could then configure his browser to reject code with unknown or incorrect signatures. A more daring user might simply want a warning. Confidence could be placed in code obtained from anywhere, even a malicious host, as long as the signature is valid and you trust the entity signing it.

Digital signatures are not a panacea, however. There are real problems with key distribution and even the smallest change in the code would require it to be re-signed. Further, although digital signatures offer protection from malicious code, there is still the possibility of bugs with security implications or other harmful effects.

Frank Stuart

[That is actually similar to the Microsoft CAPI (Cryptographic

Application

Programming Interface) concept extended to browsers. Not a bad idea.

Note: concerning hyphenating vs. hyphen-hating, notice the distinction

between re-signed and resigned. I won't resign from my crusade. PGN]

⚡ Risks of rewritable BIOSes (Valverde, [RISKS-17.96](#))

JEREMY J EPSTEIN <JEPSTEIN@mail.cordant.com>

Tue, 02 Apr 1996 15:31:18 -0500

In [RISKS-17.96](#), J.R. Valverde talked about the risks of having BIOS stored in flash RAM (because it's rewritable, I hesitate to call it ROM). A similar point was raised by Martin Portman in [RISKS-17.58](#), with related information by Sean Reifschneider in [RISKS-17.61](#). All of these are quite accurate as to the problem. The purpose of this posting is to let people know what's happening to fix the problem.

As part of a project I'm working on, I've been working with some of the large PC vendors. What I've found is that virtually all Pentium based PCs on the market today have the flaw described. This sort of problem was almost unknown in the 286/386/486 generations of PCs, which used real ROM for storing the BIOS.

Some of the hardware manufacturers understand the risk here, and have started to address it. One solution adopted by some vendors is to build a

one-way switch in hardware. Once the switch is "thrown" (by sending commands to a device on the board), the write signal to the flash ROM holding the BIOS is disabled until the next power cycle. Some vendors have put code in their BIOS to automatically throw the switch before they boot from the floppy or hard drive. This prevents any sort of malicious software from modifying the BIOS. To allow BIOS updates to occur, the BIOS looks for a "signature" on the floppy before throwing the switch, and if the signature is found it doesn't throw the switch. (The ease of spoofing the signature is another topic.)

Other vendors have implemented a BIOS modification password, which must be written to a particular address before the write signal to the flash is unlocked. Unfortunately, such a password is usually subject to a dictionary attack by the malicious software, which would be invisible to the user.

The good news is that because each vendor has solved the problem differently, it would be difficult for a virus writer to disable arbitrary PCs (although they might be able to disable all PCs from a given vendor). That is, diversity results in resistance to plague.

The bad news is that even for those vendors who are doing a good job addressing this problem, they can't retrofit machines already in the field, since it requires a hardware change that isn't economical. Further, because there's no way to tell by physical inspection whether a given machine has a rewritable BIOS, users can't determine whether they're at risk.

Vendors are reluctant to disclose how they've solved this problem (if at all), which makes it impossible for users to tell if they're at risk.

Of course the whole problem occurs only because most PCs don't run modern operating systems that would prevent a virus from directly accessing the hardware. For example, a PC running UNIX, OS/2, or NT is immune to these sorts of viruses except at boot time (which can be addressed using careful procedures).

⚡ Re: "This is not a bug" messages: MacsBug (Rafn, [RISKS-17.92](#))

David A. Lyons <dlyons@netcom.com>
Thu, 21 Mar 1996 01:46:45 -0800

Mark Rafn's message in [RISKS-17.92](#) reminded me of a change I made to the low-level debugger MacsBug, during development of Macintosh System 7.5.

If the user holds down the Control key during startup, the debugger intentionally seizes control and says "User break at <useless address>." Users who aren't expecting this write up bug reports that say "The system crashes when I hold down the control key during startup."

After the third or so of these reports, I was tired of saying "it's a feature" and decided to make the situation clearer to the users. Now the message reads:

Welcome to MacsBug (Thank you for holding down the Control key)

The bug reports stopped. Perhaps this message shows an appropriate degree of respect for the user (some alternate versions I considered showed less).

✶ Re: The Queen's Speech

Allan Engelhardt <allane@parallax.co.uk>

Tue, 2 Apr 1996 12:03:06 +0100

The Electronic Telegraph (<http://www.telegraph.co.uk/>) reported that the sentence mentioning the Polish Jews were in the electronic version of the Queen's speech and in the printed copy that was used for proof reading.

However, the version the Queen was reading from when she gave her speech was printed in a bigger font and the sentence "fell of the bottom of the page".

The RISKS are obvious.

--- Allan.

[Also noted by "timothy (t.j.) hewson" <hewsot@bnr.ca>.

But Europeans already use longer paper, so one (silly) approach might

be to proof-read in the U.S. and print the final copy in England?

Oh, yes, lawyers like long paper too, but let's keep them out of it,

or the Queen couldn't afford it. PGN]

⚡ Re: Notes on e-mail: Use of diaeresis

Dan Hicks <danhicks@millcomm.com>

Tue, 02 Apr 1996 00:43:10 -0600

This article brings to mind the birth of the daughter of a teammate of mine.

Seems the chosen name of the child was Zoe (with diaeresis over the "e").

So my teammate sent around a note announcing this name.

However, shortly

after the note went out, people started asking him why in the world he'd

named the kid "ZoK".

Turns out that e-diaeresis is mapped as ctrl-K (or is it alt-K?) on our

system. When the message was sent to other systems, however, the mail

software converted text that looked something like "Zo^K" to read simply as

"ZoK".

So another risk of computers is one of losing your identity -- on the day you're born.

Dan Hicks <http://www.millcomm.com/~danhicks>

⚡ Re: Notes on e-mail: Use diaeresis (Callas, [RISKS-17.96](#))

Daan Sandee <sandee@Think.COM>

2 Apr 1996 16:20:16 GMT

The deficiency of this proposal is demonstrated by the fact that it arrives

on my screen as "co=F6perate", "na=EFf", and "Bront=EB.". My

system is set up to properly handle ISO 8859-1, which is the only reasonable extended character set standard for use on the Internet. It was already mangled in the RISKS posting (I checked), and as far as I can guess it was presumably mangled before it left Jon's machine. I wish people wouldn't assume that the way their machine handles non-ASCII characters is the same as everyone else's.

Usenet (at least NNTP) is generally 8-bit transparent, and any European soc.culture group will tell you that ISO 8859-1 usually works, though some people's newsreaders may have to be told about it. This post of mine, however, goes out by e-mail (SMTP) and upper bits will be stripped, so I can't demonstrate its use.

|> [Not a bad idea for folks who can deal with diaeresis, but
|> there are still lots of problems that does not handle. PGN]

Well, I can handle diaereses all right, as long as they arrive in a form recognizable by my software.

Daan Sandee
sandee@think.com
Burlington, MA

[Also commented on by Malcolm Vincent <m.vincent@qub.ac.uk>.
PGN]

On the meaning of "email"

Clive Feather <cdwf@cityscape.co.uk>

Tue, 2 Apr 1996 12:14:04 +0100 (BST)

... the Oxford English Dictionary has a citation from 1480:
emailed: arranged in net or open work

Presumably we can back-form "email" from this.

Clive D.W. Feather, Managing Director, CityScape Internet
Services
cdwf@cityscape.co.uk +44 1223 566950 Fax: +44 1223 566951

[Mark Brader notes that this is in the Jargon File / New
Hacker's

Dictionary, edited by Eric Raymond. From version 3.3.3 of the
Jargon File:

``Oddly enough, the word `emailed' is actually listed in the
OED;

it means "embossed (with a raised pattern) or perh. arranged
in a

net or open work". A use from 1480 is given. The word is
probably

derived from French `emaiill'e' (enameled) and related to Old
French `emmaille"ure' (network). A French correspondent tells
us that in modern French, `email' is a hard enamel obtained by
heating special paints in a furnace; an `emailleur' (no final
e) is

a craftsman who makes email (he generally paints some objects
(like, say, jewelry) and cooks them in a furnace).'

Thanks. That only strengthens my argument for e-mail or E-
mail! PGN]

Browser return e-mail addresses

Walter Roberson <roberson@hamer.ibd.nrc.ca>

Sat, 16 Mar 1996 16:19:13 -0600

I recently received an e-mail reply that addressed someone else
by name

about a topic I've never dealt with. My system logs did indicate that I'd e-mailed the person earlier in the day, so I figured that I had replied to a posting of theirs and forward a copy to them, and that they had replied to the wrong message. I was, though, unable to find any previous postings by that author, and so concluded that it had simply been so recent that the search engines had not catalogued it yet.

After a day or so I finally realized what had happened. I had, a few weeks prior, visited another site and had needed to send e-mail out from a WWW browser on the lab computer I was using. I had configured my e-mail address as the return address, and had given my server's address as the SMTP gateway. I did not remember to de-configure them when I left, so the next time someone send e-mail from that system's browser it not only claimed to be me but also showed up in my server's logs.

So if you are using a lab computer, be sure to check the reply address before starting to send mail. If you are replying to someone who might have been using a lab computer, make sure the reply address matches your expectations.

Walter Roberson

roberson@ibd.nrc.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 18: Issue 2

Tuesday 9 April 1996

Contents

- [The weakest link: Social \(In\)security Administration](#)
[Sean Reifschneider](#)
- ["Jail Gives Hackers a Lesson in Reality"](#)
[PGN](#)
- [Australian Insurance Company and Database](#)
[Andrew Waugh](#)
- [De facto Daylight Savings](#)
[Matt Welsh](#)
- [Re: Teen Accused of Hacking](#)
[William Ehrich](#)
- [Microsoft Exchange helpfully misdirects e-mail](#)
[John Hoffmann](#)
- [Re: Notes on e-mail: Use diaeresis](#)
[Tim Pierce](#)
[Otto Stolz](#)
- [CompuServe's "secure login protocol": two steps forward, one back](#)
[Heinz-Bernd Eggenstein](#)
- [IBMMAIL e-mail address woes](#)
[Erik Naggum](#)
- [Re: X-Confirm-Reading-To: Pegasus woes on mailing lists...](#)

[Peter Yamamoto](#)

● [The risks of .forward](#)

[Christophe Beauregard](#)

● [Re: Wrong approach to Java security](#)

[Andrew Berman](#)

● [Re: Risks of rewritable BIOSes](#)

[Jeremy J Epstein](#)

[Nicholas C. Weaver](#)

● [Re: Computers, Freedom and Privacy '96](#)

[Shabbir J. Safdar](#)

● [Info on RISKS \(comp.risks\)](#)

✶ The weakest link: Social (In)security Administration

Sean Reifschneider <jafo@tummy.com>

Sun, 7 Apr 1996 22:12:30 -0500 (CDT)

The URL "http://www.nando.net/newsroom/ntn/info/040696/info5_14984.html"

reports "one of the biggest breaches of security of personal data held by the federal government". Apparently several employees of the Social Security Administration sold information including SSNs and mother's maiden names of more than 11,000 people to a credit-card fraud ring.

The fraud ring was able to use this information to activate cards which were stolen from the mail. Citibank had implemented a scheme which required customers to "activate" their credit cards when they receive them by calling a phone number and providing personal information like their mothers maiden name.

It seems that while systems are being designed to protect our property, it's just causing the crime to move closer to the person. If someone steals your credit card from the mail or your car from the parking lot, you're probably at a safe distance. Instead, they are forced to carjack your car at a stoplight because of your alarm system, or find out personal information about you.

Similarly, I heard about home breakins on alarmed houses in which the burglar would regularly trigger the alarm and be careful to leave no traces. Once the police stopped coming (because the alarm was faulty), they were free to break in and swipe whatever they like.

No matter how secure the system, the weakest link can be the clerk who's paid \$12K/year to work on the system. It doesn't take much money to convince this person to hand out our personal information.

This sort of thing kind of makes the hassle I went through in keeping my SSN from my insurance company. If you've never tried it, for me it was a huge hassle... Apparently, all of my claims needed to be handled by hand by one of the supervisors. Of course, if everyone did it, their \$4/hour clerks could take care of it.

Sean Reifschneider, Inimitably Superfluous <jafo@tummy.com>
URL: <<http://www.tummy.com/xvscan>> HP-UX/Linux/FreeBSD X11 scanning software.

[Also noted by Monty Solomon <monty@roscom.COM> quoting from Edupage,
and WOODWARD@BINAH.CC.BRANDEIS.EDU (Beverly Woodward), who

cited the

article in "U.S. Workers Stole Data on 11,000, Agency Says"
in

The New York Times, 06 Apr 1996, p. 6, from which most
other
reports seem to have been drawn. PGN]

✶ "Jail Gives Hackers a Lesson in Reality"

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

Mon, 8 Apr 96 18:45:15 PDT

Terry Ewing (now 21, with 21 months in federal custody ahead of
him)

downloaded 1,700 credit-card numbers off of a Tower Records
computer system,

just before leaving for DefCon, the West Coast "hackers"
convention". His

friend Michael Kim (now 20) is facing an 18-month sentence.

Apparently,

Tower folks knew their systems had been under attack previously,
and were

monitoring misuse. Police encouraged Tower to wait for the next
attack --

in which the intruders used the Tower computer to sort the
captured

credit-card numbers by expiration date and create a file of
those with a

date at least a year away -- while being observed. Agents
tracked the

intrusion to their apartment, which was searched, revealing the
purloined

information. The two young men were convicted of a felony,
although they

had not profited from the credit-card numbers. [Source: *San
Francisco

Chronicle*, 8 Apr 1996, p.A2.]

The article concludes with a quote from Mike Godwin of EFF
about those

who ``have this myth that they are cool guys, and [that] the cool guys always win over the suits. But the fact is that they are half-socialized, post-adolescents with serious ethical and moral-boundary problems.''

[Stores should not store credit-card numbers, but I guess we can no longer number the stores that do not behave sensibly. I just asked a mail-order outfit if they would keep a card number around for a long-deferred delivery; the answer was, ``yes, but we keep in a place where no one can access it.''

I am sure that gives you RISKS readers a lot of comfort. PGN]

✶ Australian Insurance Company and Database

Andrew Waugh <A.Waugh@mel.dit.csiro.au>
Sat, 06 Apr 1996 15:07:33 +1000

The 6-7 Apr 1996 edition of 'The Weekend Australian' carries a report (p 5) on a court case involving the large Australian insurance company AMP and an attempt to build a large database of all Australian households.

It was alleged that the "massive database... was supposed to identify every household in Australia, give each household a unique identifier number, detail the dwelling type of each household - whether it was two-story, weatherboard [timber] or brick - and also detail the fire, storm and flood risk rating of each home." The contractor developing the

database, Indata,
expected this database to give AMP a significant commercial
advantage.

This database was alleged in court to to have been based on a
magnetic tape
of the Australian electoral roll. Under the Australian Electoral
Act,
magnetic tapes of the electoral roll cannot be obtained for
commercial
purposes. The former manager of Indata said that he had assumed
AMP had
investigated the legalities of purchasing the tape and that
Indata and AMP
were acting within the law. The tape had already been purchased
before the
manager joined Indata.

The court case is a committal hearing against a former AMP
client manager
who is charged with 12 counts of attempting to defraud AMP. The
fraud
involves payments to Indata totalling \$324,809 (Aus). AMP is
expected to
claim that was not aware of the illegal purchase of the
electoral roll and
that their client manager had inappropriately authorised payment
to Indata.
AMP has demanded return of the money.

The committal hearing will continue next month.

andrew waugh

De facto Daylight Savings

Matt Welsh <mdw@CS.Cornell.EDU>

Sun, 7 Apr 1996 13:31:38 -0400

At <http://www.timing.se/Daylight.html> there is a brief discussion of the rules for Daylight Savings Time changeovers for central Europe and the UK. At the end of the page it says:

```
> NOTE: From autumn 1996 the rule of changing from standard time
to
> daylight time is changed. The new rule is valid for central
Europe
> including the UK is:
>
> Standard time      to Daylight Saving      LAST SUNDAY OF MARCH
> Daylight Saving   to Standard time      LAST SUNDAY OF
OCTOBER
>
> The rule is a "de facto standard," not a law.
>
> The switching occurs at 01:00 UTC for central Europe
(Stockholm Paris etc.)
> Local time that is at 02:00 STD to DST  and  03:00 DST to STD.
> (STD = Standard time, DST = Daylight Saving Time or Summer
Time.)
>
> Note: The legal switching is steered by laws that state dates
for a couple
> of years. When a period ends a new law is issued that gives
the dates for
> the next years.
>
> The Laws do not state any general rule. Only dates for a
couple years
> each time. The "de facto rule" works, but there is no warranty
it will
> work forever!
```

With all of our scrambling about to deal with the Year 2000 problem, shouldn't we be just as concerned with this inconsistency that arises yearly (especially if there are no 'hard and fast' laws/standards to dictate DST changeovers)?

M. Welsh, mdw@cs.cornell.edu

✉ Re: Teen Accused of Hacking

William Ehrich <ehrich@minn.net>

Sat, 6 Apr 1996 11:32:31 -0600

If my bank kept my money in a cardboard box in their parking lot and children stole it, I would blame the bank before the children. As long as corporations and institutions design their computer systems only for convenience and least cost, with maybe a superficial gesture at something called 'security', they won't solve the problem.

The biggest risk of all is from people who won't accept their responsibility.

- William Ehrich

✉ Microsoft Exchange helpfully misdirects e-mail

John Hoffmann <john@netweave.com>

Mon, 8 Apr 1996 11:40:21 -0400

Like most e-mail clients, Microsoft's Exchange allows you to maintain lists of user's addresses along with aliases. In our simple configuration, we have two, a personal list and a global list. Up until recently, since our e-mail system was closed and limited to project members, my personal list was almost empty. Since we have added an Internet gateway, I've

begun

adding addresses not on the global list to my personal list.

Exchange has another useful feature as well, it will expand names from just the first characters. If multiple names match the abbreviation, it will ask you to pick one.

Today I sent out an internal message, using "schu" as an abbreviation for schumacher, which I have done many times in the past. Shortly there after the message was returned from the AOL e-mail daemon as undeliverable, highly surprising since it was an internal message not destined for the Internet.

It turns out that last week I incorrectly added an AOL user whose name also begins with "schu" to my personal address list. Exchange apparently only checks one list at time, flagging multiple possibles only within the list. In this case, it checked my personal list first, matched the AOL user, and quietly sent the message on. If the name at AOL had been correct, I would have not known about the misdirection at all.

The risks are obvious - instead of a somewhat trivial and incomprehensible internal message, the message could have been highly confidential or time critical. The solution is trivial as well - check all mail lists for conflicts (or at least have that as the default configuration & easily selectable).

✶ Re: Notes on e-mail: Use diaeresis (Sandee, [RISKS-18.01](#))

Tim Pierce <twpierce@midway.uchicago.edu>

Fri, 5 Apr 1996 19:09:29 GMT

>Usenet (at least NNTP) is generally 8-bit transparent, and any European
>soc.culture group will tell you that ISO 8859-1 usually works, ...

Though many machines on Usenet are eight-bit clean, NNTP is defined to be seven-bit. There's no guarantee that the use of raw characters in ISO-Latin-1 will come out unharmed on the other end.

More risks: assuming that an action is advisable simply because it "usually works." This, unfortunately, is becoming more and more common even among news software developers, some of whom have simply conceded the seven-bit encoding battle and now write for an eight-bit net.

✶ Re: Notes on e-mail: Use diaeresis (Sandee, [RISKS-18.01](#))

Otto Stolz <Otto.Stolz@uni-konstanz.de>

Tue, 9 Apr 1996 10:39:53 -0500

On 2 Apr 1996 16:20:16 GMT, sandee@Think.COM (Daan Sandee) said:
> [...] "co=F6perate", "na=Eff", and "Bront=EB.". [...] It was already
> mangled in the RISKS posting

Apparently, these examples were sent to RISKS encoded as "quoted-printable".

I guess, they were contained in an e-mail item adorned with the appropriate MIME headers to announce that transfer encoding to any

interested parties.

However, in the process of digesting, all header fields (except the From, To, and Subject fields) were stripped off.

This seems to be a general problem with contemporary mail-digesting software.

Of course, the transfer-encoding has to be undone before you can safely remove the pertinent header field. I hope, our moderator will be able to find a mail-digesting program that handles MIME headers properly.

> [...] I wish people wouldn't assume that the way their machine handles

> non-ASCII characters is the same as everyone else's.

This is exactly the reason MIME was invented for.

> Usenet (at least NNTP) is generally 8-bit transparent, and any European

> soc.culture group will tell you that ISO 8859-1 usually works [...]

Not quite so! There are mail transfer agents, and perhaps other intermediate software, that still will drop the most significant bit of every 8-bit character.

> This post of mine, however, goes out by e-mail (SMTP) and upper bits will

> be stripped [...]

Hence, contributions to RISKS, and other e-mail based services, must exploit

MIME to convey those characters (until, eventually, the powers that be might

agree on a 8-bit, or even 16-bit, based mail protocol). It is the digester's

duty to undo any transfer-encoding before the mail is digested, and to encode

the whole digest for transport, as necessary.

> Well, I can handle diaereses all right, as long as they arrive
in a form
> recognizable by my software.

And it will be the subscriber's duty to undo the transfer-
encoding of the
whole digest.

Otto Stolz

[I have asked several folks what I would need to do to MIME-
ify RISKS.

I get responses that it is not that easy, or that it won't
help

those who don't deal with MIME, or that perhaps I should just
wait until things settle down. Meanwhile, we have a
justification
for indigestion with undigestification. PGN]

⚡ CompuServe's "secure login protocol": two steps forward, one back

Heinz-Bernd Eggenstein <eggenste@noether.informatik.uni-dortmund.de>

Thu, 04 Apr 1996 19:34:12 +0200

Summary: a new CompuServe Information Service (CIS) logon
protocol was
designed to prevent passive and active attacks (where the
attacker
impersonates a CompuServe node) but a flawed implementation in
the
WinCIM 2.0(.1) client software still allows active attacks.

Version 2.0 of the "WinCIM" access software introduced a new
logon protocol.

Previous versions of the software had transmitted the user's UID
AND his/her
password in plaintext during logon. The risks are obvious,

especially when connecting via the Internet to CompuServe (e.g. to save long distance telephone charges).

The new, "secure logon protocol" is a challenge-response type protocol where the "challenge" is to compute a keyed hash-function, the key is derived from the shared secret, the user's password:

- 1) The client (WinCIM) generates a pseudorandom string of bits, its "nonce"
(RB)
- 2) The client transmits the user's UID (e.g. 12345,6789) and the additional parameter "/secure:1" to request a secure login.
- 3) The host transmits its pseudo random nonce (RA) (The old protocol would instead prompt for the password)
- 4) client sends RB to the host
- 5) client computes $UR := MD5(S|Z|RA|RB|S)$ and sends it to the host (where S (128 bits) is a function of the password, "|" stands for concatenation, Z is a 128bits block of 0s and MD5 is the well known message digest function.)
- 6) The host performs the same calculation with it's copy of the user's password. If the results match, the host sends $HR := MD5(S|Z|RB|RA|S)$
(Note the symmetry in the calculation of HR and UR)
- 7) The client software verifies HR with it's copy of the password to
make sure the host is really a CIS node (!)

(See the script-files cserve.scr and seclog.scr in the subdirectory SCRIPTS of a WINCIM 2.0(.1) installation, WinCim is available via anon. ftp at ftp.compuServe.com).

Weaknesses:

a) The scriptfile cserve.scr (versions 3.8 & 3.8.1) has the following bug:

even after requesting a secure logon, the client software will fall back

into the old protocol when receiving a "Password" prompt (Client: "I want

a secure logon" Host:"OK, but anyway, give me your password" Client "Well

ok then, here it is ..."). It will send the password in plaintext! This

makes the protection against active attacks (see step 7) obsolete.

b) A timeout condition or even an invalid HR response from the host will

(seclog.scr & cserve.scr version 3.8.1) restart the protocol (it won't

disconnect!), using *the same* client-nonce RB again, instead of

generating a new one. If a spoofing host can predict RB as in this

situation, it can pick the same nonce, leading to HR=UR=MD5(S|Z|RB|RB|S),

so the host can just send back UR as HR.

Note that unlike a), b) does not compromise the user's password.

There may be other ways to predict the client software's nonce e.g. *if* the PRNG used by WinCIM is predictable (this calls for further investigation).

Note that *offline* dictionary attacks to guess the password are possible

after a passive, eavesdropping attack (so you still have to pick a "good"

password). It's debatable whether CIS's password recommendation (<word><non-alphanum. char.><word>, both words unrelated, e.g. apple@battery) is adequate in this context).

I notified CIS about these weaknesses and I was informed that they are

"fixed" now, no details were given about the fix (source: Britta

Herbst,
German customer support (11111.754@compuserve.com)).

Risks? The new protocol is obviously an improvement over the old, plaintext-password-only version. It's debatable whether protection against active attacks is at all necessary for access to an online service. However, CIS itself designed it's protocol to prevent spoofing attacks. Anyway, I think this a good example how to half-ruin a good protocol by embedding it into carelessly written code.

Credits: Thanks to Gary Brown (70003.1215@compuserve.com) for sending me information on the implementation of the new protocol).

Heinz-Bernd Eggenstein [usual disclaimers]

⚡ IBMMAIL e-mail address woes

Erik Naggum <erik@naggum.no>
03 Apr 1996 13:11:21 UT

You may not know the IBMMAIL system. Internet addresses are translated to a seven-digit number, which users use instead of real addresses. It so happens that I once ran a large mailing list and needed to track down which messages were not delivered to which people, and so generated a unique Return-Path for each message. This caused a large number of IBMMAIL numbers to be assigned to such addresses. About once a month, I receive confirmations of business transactions between Hong Kong and Singapore companies to one of these addresses. Clearly, the RISK is that humans

mistype numbers all the time, and when the addresses in a given range are all valid, will send mail to the wrong recipient every now and then, just as people misdial telephone numbers.

All information expressed in long numbers whose accuracy matter to either party include redundant digits to reduce the number of valid numbers and to provide consistency checks. The same should be true of IBMMAIL numbers.

(Indeed, it should perhaps be true of domain names and usernames, too.)

#<Erik>

⚡ Re: X-Confirm-Reading-To: Pegasus woes on mailing lists...

Peter Yamamoto <pjyamamo@daisy.uwaterloo.ca>

Thu, 4 Apr 1996 10:42:36 -0500 (EST)

> Recently, on a mailing list I maintain, a Pegasus (the name of a
> Mac/Windows e-mail reader) user posted a message with a line:
>
> > X-Confirm-Reading-To: <e-mail address>
>
> This would be fine if Pegasus respected the field value when
> acting on
> the presence of this field. But Pegasus programmers
> apparently took the
> RISK of assuming that they didn't have to. Now every list
> member using
> Pegasus is generating a confirmation message to the list.

Well, the problem wasn't as simple as that, that is only what it looks like...

The "problem" is due to a new release of Pegasus which added a directed confirmation header field as well as keeping the old confirmation header field (which old versions simply respond to as best as they can). The new field name is called X-Confirm-Reading-To: <e-mail address> and the old name is "X-pmrqc: 1".

Hence, unless familiar with these things, the mailer looks like it is not behaving.

There are Risks in this whole episode, but I've worn myself thin trying to defend the meaning of my post to a listserv listowner's list (a warning of disruptive behaviour) with the author of Pegasus who took my comments differently (as a rude personal attack).

Peter

⚡ The risks of .forward

<cpbeaure@undergrad.math.uwaterloo.ca>

Tue, 2 Apr 1996 11:12:20 -0500 (EST)

Standard procedure for us net types is to leave .forward files when we change accounts. This is what I did when I left my previous employer.

Because of the nature of the Internet firewall we had there, to access the net users had to actually log into the firewall machine - a bad idea in itself, but it gets worse.

One fine day, I logged in to find a message informing me that the firewall password had changed. Conveniently, the message also included the new password. It seems that when I left, not only had they not erased the .forward file, but they hadn't removed me from the system alias file.

The risks?

- 1) Clean up after your old employees.
- 2) E-mail goes everywhere.
- 3) Don't e-mail passwords. Ever.

✶ Re: Wrong approach to Java security (Stuart, [RISKS-18.01](#))

Andrew Berman <aberman@cs.washington.edu>
Fri, 05 Apr 1996 16:59:49 PST

>In [RISKS-17.95](#), Jacob Palme suggests that the reputation of "well-kept depositories" and PICS-like ratings can be used to guard against malicious Java code. A more useful idea along the same lines is to allow for code to carry a digital signature. ...

Neither PICS-like ratings nor Digital Signatures is going to solve the problem. Yes, they might constrain some malicious users. But what about the data loss from buggy software? Also, decentralization of code is a promise of web-based languages. A world in which every piece of code has to be checked against a database of signatures is a much less flexible world

than one in which code runs in a "safe" environment.

Not to mention that a digital signature for a company will undoubtedly be known by more people than a digital signature for a single user. Thus, the opportunities for theft of the signature would increase dramatically.

Andrew P. Berman Dept. Of Computer Science, University Of Washington
aberman@cs.washington.edu | <http://www.cs.washington.edu/homes/aberman>

⚡ Re: Risks of rewritable BIOSes (Epstein, [RISKS-8.01](#))

JEREMY J EPSTEIN <JEPSTEIN@mail.cordant.com>
Tue, 09 Apr 1996 09:58:42 -0500

After my posting in [RISKS-18.01](#), several people sent me e-mail. A few clarifications to my original note:

* Some PC vendors have a jumper that disables writing the flash. In my experience, this is unusual, although it's clearly present in some cases. For those who are lucky enough, the jumper is even documented. Clearly this is a good solution for those whose PCs have the option. Of course most users won't read the manual that comes with the PC and thus won't realize that there's a risk, much less understand how to thwart it. [Pointed out by mark@leasion.demon.co.uk (Mark Evans) and afelson@milton.ecte.uswc.uswest.com (Adam Felson).] [AND also by "Nicholas C. Weaver" <nweaver@CS.Berkeley.EDU>, with the default being disabled -- see the next item. PGN]

* I wrote "...each vendor has solved the problem differently..." The word "vendor" should be understood as the vendor of the motherboard, which may not be the same as the PC vendor. That is, a brand X PC may use a brand Y or brand Z motherboard. So looking at the outside of the case may be insufficient to determine whether the PC is "safe". [Pointed out by Mark Evans.]

* As an aside I wrote that the risk would be eliminated if people used more modern systems such as UNIX, OS/2, or NT. As pointed out by Benedikt Stockebrand (benedikt@devnull.ruhr.de), it doesn't **eliminate** the risk, because there may be bugs that allow subverting the system and thus gaining access to the flash RAM. Stockebrand also pointed out that (on UNIX systems) if you can get the virus/trojan run by root, then all bets are off. Perhaps I should have said that running a more modern system **reduces** the risk, since a virus/trojan would have to be a lot smarter than in a DOS/Windows environment.

The above notwithstanding, the point stands: most Pentium-based PCs are extremely vulnerable to flash-based attacks.

✶ Re: Risks of rewritable BIOSes (Epstein, [RISKS-17.81](#))

"Nicholas C. Weaver" <nweaver@CS.Berkeley.EDU>
Fri, 5 Apr 1996 10:52:40 -0800

Although I believe software solutions are necessary for correcting the flash-BIOS problem on existing motherboards, I think all future motherboards should just resort to an old-fashioned physical jumper. If the jumper is in place, then the BIOS is reprogrammable. (If a malicious person has access to your motherboard, he/she can do a LOT more damage than simply reflashing the BIOS, but a malicious program can't -- especially if the motherboard is shipped without the jumper in-place.)

✶ Re: Computers, Freedom and Privacy '96 ([RISKS-18.01](#))

"Shabbir J. Safdar" <shabbir@panix.com>

Sat, 6 Apr 1996 15:59:55 -0500 (EST)

My RISKS commentary about the Bruce Sterling piece at CFP '96 drew many pieces of e-mail. You can get a RealAudio recording of it from

URL:<http://www.w3.org/pub/WWW/CFP4/live.ram>

(I don't have a RealAudio player on this machine, so I cannot verify that it works..)

The live version left me feeling numb and panicky.

[oram@unixg.ubc.ca (John Oram) reported that the audio version of the entire CFP 96 is available for your listening pleasure "(in the bandwidth-conserving RealAudio format)" at:

<http://swissnet.ai.mit.edu/~switz/cfp96/> .]



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 18: Issue 3

Wednesday 10 April 1996

Contents

- [Intel shutdown by power company software bug](#)
[Bruce E. Wampler](#)
- [Daylight Savings Time problem](#)
[Bruce E. Wampler](#)
- [Re: De facto Daylight Savings](#)
[Dik T. Winter](#)
- [Don't go it alone -- the Risks of poor design decisions](#)
[Russ Broomell](#)
- [Warning! My \[...\] let me \[dangerous/confidence-breaking act\]](#)
[Rob Bailey](#)
- [Signing binaries](#)
[Bennet Yee](#)
- [Re: Jury Duty](#)
[D.C. Sessions](#)
- [Secure authentication falling back to insecure](#)
[Tim Kolar](#)
- [Re: Notes on e-mail: Use diaeresis](#)
[Jim Rees](#)
- [Re: Microsoft Exchange helpfully misdirects e-mail](#)
[Anthony Atkielski](#)

[Steve Sapovits](#)

● [COMPASS '96 Advance Program](#)

[Connie Heitmeyer](#)

● [The Second USENIX Workshop on Electronic Commerce: cfp](#)

[Bennet Yee](#)

● [Info on RISKS \(comp.risks\)](#)

⚡ Intel shutdown by power company software bug

<wampler@cs.unm.edu>

Wed, 10 Apr 1996 11:50:05 -0600 (MDT)

>From April 9, 1996 Albuquerque Tribune:

Computer-chip-manufacturing operations at Intel Corp.'s Rio Rancho plant were back to normal today after a five-hour power failure, the company said. Intel Corp. spokesman Richard Draper said today that Monday's power failure, which ruined an undisclosed number of chips, including some of the plant's Pentium microprocessors, was caused by a malfunction of Public Service Company of New Mexico software. "For business reasons, we're not going to provide exact numbers as to the product loss from the shutdown," Draper said. "However, the power outage won't have significant impact on Intel or its earnings. It's expensive, but again, it's not a significant impact on our bottom line." Draper said the power failure occurred about 9 a.m.

Monday; full power was restored about 2 p.m. Monday.

Intel evacuated about 600 workers during the outage because of dark and potentially unsafe working conditions. "The PNM people told us it was a

glitch in a switching system," Draper said. "The original glitch lasted a few seconds, but we waited to start operations because we were uncertain about what happened and wanted to make sure we could restore full power."

Draper said PNM's apparent software error is believed to have caused the wrong circuit breaker to open at a substation, incapacitating three of six transformers.

Karin Stangl, a Public Service Company of New Mexico spokeswoman, said power was restored after about a minute, and she could not explain the longer problem at Intel. Stangl said PNM and Intel are investigating.

[I find Intel's conservative response, both in evacuation, and waiting to be sure the power was back, interesting.

Maybe the software was running on a non-Intel processor trying to get even with the Pentiums... BEW-are]

Bruce E. Wampler, Ph.D., Adjunct Professor, Department of Computer Science,
University of New Mexico wampler@cs.unm.edu <http://www.cs.unm.edu/~wampler>

⚡ Daylight Savings Time problem

<wampler@cs.unm.edu>

Wed, 10 Apr 1996 11:31:07 -0600 (MDT)

I was hit by a daylight savings time problem Monday, the day after the time

changed here. My machine is running four different operating systems:

Windows 95, Windows NT, OS/2, and Linux. Since I'd doing cross platform

development, I usually boot at least two different OS's a day.

Monday, I booted Windows 95 first. At startup, I was greeted by a polite messages asking if the time should be changed to DST. Fine. Time changed and correct.

Later in the day, after booting both NT and Linux, I noticed the time was yet another hour ahead. Either NT or Linux (and I suspect NT, but can't confirm that) had also, but invisibly, changed to DST.

After some thought, and a class discussion in the software engineering class I teach, I've concluded this is not an easy problem to solve. In this case, there were two basic contributing factors I can figure out. First, PCs keep the internal clock in local time. Not a good idea -- it should be Universal Time -- but reality. The problem is then that NT or Linux made the assumption it was the only OS on the machine, and was free to update the time. Unlike Win95, which could be polite about the change because it is normally a single user system, NT and Linux both could reasonably assume they don't normally get shut down each evening, and thus the silent time update (I'm guessing). It would be unreasonable to expect confirmation from an operator.

In this case, however, the time update did come at boot time. It seems to me a better update policy for NT/Linux would be to silently update the time if the change happened while running, and require a confirmation if it happens at boot time. Not perfect, but better. I tried OS/2, also, and it just

ignored the time change.

Bruce E. Wampler, Ph.D., Adjunct Professor, Department of
Computer Science,
University of New Mexico wampler@cs.unm.edu <http://www.cs.unm.edu/~wampler>

✶ Re: De facto Daylight Savings

Dik T. Winter <Dik.Winter@cwi.nl>
Tue, 9 Apr 1996 22:08:02 GMT

> At <http://www.timing.se/Daylight.html> there is a brief
discussion
> of the rules for Daylight Savings Time changeovers for
central Europe
> and the UK. At the end of the page it says:
...
> > The rule is a "de facto standard," not a law.
...
> With all of our scrambling about to deal with the Year 2000
problem,
> shouldn't we be just as concerned with this inconsistency
that arises
> yearly (especially if there are no 'hard and fast' laws/
standards to dictate
> DST changeovers)?

But there *are* 'hard and fast' laws that dictate DST
changeovers. There is
however *not* a law that dictates this far into the future but
only for a
few coming years. (Note that these laws, EU directives, are
made up far in
advance. It was already known a few years ago that the EU would
change the
rule this year.) It appears not to be very advisable to cast
changeover
dates in concrete. It is up to the software to deal with this

flexibility

and Andrew Olson's timezone package deals very well with it.

(And some

software does not handle it well at all. Most annoying was a bug in SGI's

software which thought the last Sunday in September last year was October 1,

and so switched out of DST one week late. Exactly the same bug stroke again

this time when the software thought that the last Sunday of March was March

24, and so switched into DST one week early. Surprising that the bug was

not fixed in that half year.)

dik t. winter, cwi, kruislaan 413, 1098 sj amsterdam,
nederland, +31205924098

home: bovenover 215, 1025 jn amsterdam, nederland; <http://www.cwi.nl/~dik/>

✶ Don't go it alone -- the Risks of poor design decisions

"-Broomell, Russ" <MARKETING/MARKETING/RUSS%Konica_Imaging@mcimail.com>
Wed, 10 Apr 96 15:21 EST

I have read posts recently about several risks that all boil down to one thing -- the Risk of making poor information system design decisions.

Poor security systems, employees selling data, even the CDA are all at

least partly the result of poor technical decisions.

Unfortunately, this

often happens in low-bidder-gets-the-job situations.

Konica, the company I work for, has come up with a partial solution to

this problem. We formed a group called the Information Partners, a

cross-functional group of technical people, managers, and end

users from
across our company. This group steers our corporate information
and
technology resources. We serve as an interface between
programmers, users
and upper management, and frequently call in outside help to get
the best
systems at reasonable prices.

NOTE: I am not representing Konica as good, bad or otherwise,
just stating
how one group met a Risk.

Our solution has its own Risks, but we help to highlight
the importance
of technology in a business environment. This usually gets us
away from the
lowest-bidder reasoning. The key to success seems to lie in not
getting
bogged down in the committee mentality, but rather contributing
where we can
add something. Is a committee the answer to every problem?
Certainly not,
but where computers and systems are concerned, more input can
mean a better
result.

⚡ Warning! My [...] let me [dangerous/confidence-breaking act]

<wm8s@citynet.net>

Wed, 10 Apr 1996 02:18:50 -0400

I've seen hundreds of stories here and elsewhere about software,
hardware,
hybrid and other systems that get blamed for dangerous actions,
actions which
compromise security or confidential information, etc., and then
always end
with the standard "risks are obvious" caveat. So I thought I'd
relate a

description of a tremendous danger I just discovered right here in my own residential neighborhood.

There's a partly computer-controlled / partly operator-controlled mechanical system near my house that must weight a couple of thousand pounds and has what I consider to be an unacceptably dangerous user interface.

Today, I noticed that the operator had the ability to operate the system in a manner that was in violation of numerous laws -- local, state and federal -- without any type of lockout mechanism built in, that there were essentially NO facets of the user interface that were designed to preclude (or even hamper) the operator from exceeding the system's absolute maximum operating parameters (leading quickly to a complete, catastrophic and dangerous failure of the system), and that the system could be easily operated in a manner which very seriously jeopardized the safety of the operator and anyone else within a mile or two (easily fatally), all without even the slightest intervention by the control system's software or hardware.

Of course... it's my car. My point is that, yeh... your software can make it *easier* for you to send a confidential memo to your lover and dirty pictures to your boss, or a Man-Machine Interface can make it *easier* to land a plane down with the landing gear up, or an engineer can crash a locomotive into the station *quicker* because the signals weren't triple-redundant and both warning lights had burned out...

But *YOU'RE* the one that didn't carefully review the address

list on that
memo before you clicked [SEND], and *YOU'RE* the one that didn't
religiously
observe the standard landing checklist, and *YOU'RE* the one
that should have
realized that you shouldn't be going 65 MPH 100 yards from Grand
Central.

I'm not trying to defend my profession; I've cursed up and down
many a poorly
designed system. But I wonder: are we trying to build better
MMI's or just
encouraging dumber operators to distance themselves from
responsibility for
their own actions?

Rob Bailey, Bailey Computer Systems Kanawha / Charleston
WM8S (wm8s@citynet.net) Radio Amateur Civil Emergency Service

✶ Signing binaries (Palme, [RISKS-17.95](#))

Bennet Yee <bsy@Play.UCSD.Edu>
Sat, 6 Apr 1996 14:58:35 -0800

In [RISKS-17.95](#), Jacob Palme suggested the use of peer-review to
filter out
malicious software. While potentially useful, there are a wide
variety of
attacks such a strategy would likely miss. For example, suppose
a virus /
alternative-model-Java applet author specifically targetted
machines which
were in a particular domain. Such a form of malicious software
is much less
likely to be detected by however large a user pool. (And a
virus targetting
a single company has been found ``in the wild'' before, I
believe.) It is
risky to believe that our past experiences with malicious

software is a completely accurate predictor of the future; riskier still not to consider the entire collective past experience.

The idea of signing software is not new. Bellcore's Betsi system uses PGP to have the author sign their software, and the idea has certainly been bounced around the security community before that was implemented. The effect of CAPI signatures is to make governmental agencies happy so that the API may be exported. I doubt that Microsoft cares very much whether the cryptographic service provider code written by third parties are bug free. In the CAPI signing model, it is a central authority doing the signing. Certainly there might be liability issues if MS -- or Sun/ Netscape/... for centrally signed Java applets -- says anything about having looked cross-eyed at the third party code (risks of deep pockets?).

With author-signed code, the picture wouldn't be entirely rosy either. Given the number of potential individual coders on the 'net, the process of knowing who writes good code and who writes buggy code (and potentially cause security problems) is rather daunting.

✶ Re: Jury Duty

"D.C. Sessions" <dc.sessions@tempe.vlsi.com>
Tue, 02 Apr 1996 12:18:08 -0800

Governments aren't the only organizations that make stupid database-key decisions. Our prescription-drug plan has limitations on how

much of a given drug a patient can get at a time -- generally one month's supply. A reasonable restriction, all in all, and especially so with Federally controlled substances such as Ritalin and Dexedrine.

The trouble is, their computer systems check this by keeping a history of each patient's prescription fills. The primary database key is the plan number (basically the primary beneficiary's SSN) and the secondary key, to distinguish family members, is the individual's birthdate. (Anybody see the problem here?)

We have identical twins. Both are on similar long-term medications for asthma and ADD, which routinely sends the pharmacy nuts because they can't get approval for the second set. (A related problem would be if both parents were covered, thus having different primary keys. Why do I suspect that THAT problem was resolved early?)

The RISK here is in programming for the 95% case without any provision for not-all-that-rare exceptions.

D. C. Sessions dc.sessions@tempe.vlsi.com

🔥 Secure authentication falling back to insecure ([RISKS-18.02](#))

Tim Kolar <tkolar@cisco.com>
Wed, 10 Apr 1996 09:27:55 -0700 (PDT)

In [RISKS-18.02](#), eggenste@noether.informatik.uni-dortmund.de

wrote to explain security problems with CompuServe's new client. One of the major ones was that, although they had switched the primary authentication to do a challenge handshake, the client would still happily accept a request for plaintext authentication.

This actually turns out to be a relatively common problem with PPP client implementations. There are a number of public domain and commercial clients that will accept a PAP negotiation even if configured only for CHAP. Security nightmare.

It seems to me that this mistake flows very naturally out of the PPP specification as a whole. A good PPP implementation will attempt to negotiate just about anything -- Ask for X, if they refuse, ask for Y, if they refuse ask for Z -- and that same implementation will be as generous as possible in accepting options -- Sorry, we don't do X. You want to do Y? Okay.

This mindset is great for interoperability, but it's a very bad failing when it comes to security.

-Tim Kolar cisco Systems

⚡ Re: Notes on e-mail: Use diaeresis (Pierce, [RISKS-18.02](#))

Jim Rees <rees@umich.edu>
Wed, 10 Apr 1996 19:13:50 -0400

> Though many machines on Usenet are eight-bit clean, NNTP is defined to be
> seven-bit. There's no guarantee that the use of raw characters in
> ISO-Latin-1 will come out unharmed on the other end.

NNTP says nothing about character set in the text of an article. In fact, it says, "No attempt shall be made by the server to filter characters, fold or limit lines, or otherwise process incoming text" [rfc977]. I take this to mean it is intended to be 8-bit clean when used over an 8-bit clean transport, such as TCP.

USENET messages are not explicitly limited to 7-bit, but "all USENET news articles must be formatted as valid ARPANET mail messages, according to the ARPANET standard RFC 822" [rfc850]. Read literally, this excludes all non-encoded non-ascii text.

Current practice varies from one newsgroup to the next, and even within newsgroups. Some use 8-bit characters, others use some sort of 7-bit encoding, and there is usually nothing in the headers or the body to indicate what the encoding and character set are.

⚡ Re: Microsoft Exchange helpfully misdirects e-mail (Hoffman, R-18.02)

Anthony Atkielski <73064.2766@CompuServe.COM>
10 Apr 96 13:35:01 EDT

In [RISKS-18.02](#), John Hoffman (<john@netweave.com>) describes

risks that he
felt were associated with the methods used by the Microsoft
Exchange e-mail
client to resolve partial addresses in outgoing messages.

As it happens, there are two features of Exchange that can help
to avoid or
eliminate these risks: the Check Names feature, and an option in
the client
that controls the query order for address providers.

The first feature (activated by a toolbar button or Alt-K on the
keyboard)
resolves all partial addresses in a message header before the
message is
actually sent; the user may then verify that the selections made
by Exchange
actually correspond to the recipients he has in mind.

The second feature (found on the Tools | Options | Addressing
property
sheet) lets the user change the order in which address providers
are
queried. By placing the Global Address List ahead of the
Personal Address
Book (the opposite of the default) in this way, Exchange can be
forced to
look for a match within the user's organization before checking
any
(possibly external) addresses in his Personal Address Book. (As
John has
correctly surmised, Exchange stops at the first address book
that contains
one or more matches for a partial address.)

I use both of these features, and I rarely encounter any
problems with
incorrect resolution of ambiguous partial addresses. If I have
any doubt, I
do a quick double-click on the resolved name in order to verify
that it is
really pointing to the recipient I have in mind. I do try to
use display

names in my Personal Address Book that do not match anything in the Global Address List, so that I can spot incorrect resolution of an address at a glance (e.g., the display name for my own CompuServe address in my Personal Address Book is slightly different from the display name of my internal address on the Global Address List).

Anthony Atkielski

✉ Re: Microsoft Exchange helpfully misdirects e-mail (Hoffman, R-18.02)

Steve Sapovits <steves@telebase.com>
Wed, 10 Apr 1996 14:28:07 -0400 (EDT)

I haven't used this particular mailer, but maybe part of the risk is in the design of the mailer. The free UNIX mailer I use allows a long name to be assigned to an alias (e.g., the person's real full name). When I enter an alias, that name immediately appears on the "To:" line in front of me. That's saved me from embarrassment more than once. Being extra paranoid, I almost always also use a feature of the mailer that lets me see all the headers before I send a message (and change them if I've goofed). Silent mapping of aliases is not something I would want.

Steve Sapovits Telebase Systems steves@telebase.com <http://www.telebase.com>

COMPASS '96 Advance Program

Connie Heitmeyer <heimmeye@itd.nrl.navy.mil>

Tue, 9 Apr 1996 18:00:15 -0400 (EDT)

COMPASS '96

11th Annual Conference on Computer Assurance

National Institute of Standards and Technology,

Gaithersburg, MD

June 17-21, 1996

ADVANCE PROGRAM [abridged for RISKS]

Monday, June 17 (Tutorials)

Safety Case Construction and Management

by John A. McDermid (University of York, UK) -- FULL DAY

Automatic Formal Analysis of Cryptographic Protocols

by Stephen Brackin (ARCA Systems, Inc., USA) -- HALF DAY

Impact and Design of the Human-Machine Interface

by Michael Harrison (University of York, UK) -- HALF DAY)

Tuesday, June 18 (Tutorials)

ACL2, An Extended Reimplemented Version of Nqthm Logic

Theorem Prover by J Strother Moore and William D. Young

(Computational Logic, Inc., USA) -- FULL DAY

A Framework for Reasoning About Assurance

by Jeffrey R. Williams (ARCA Systems, Inc., USA) -- HALF DAY

Wednesday, June 19

8:45 am--Welcome and Keynote

Welcoming Remarks: Karen Ferraiolo, General Chair

Stuart Faulk and Connie Heitmeyer, Program

Chairs

Keynote Address I

"The FAST Process (Family-Oriented Abstraction, Specification and Translation)--A Study in Successful Technology Transfer"

David Weiss (Lucent Technologies, Bell Laboratories, USA)

10am--Formal Specification and Analysis I

"Table Transformation Tools: Why and How"

H. Shen, J. Zucker, D.L. Parnas (McMaster University, Canada)

"Simulation vs. Verification: Getting the Best of Both Worlds"

Aloysius K. Mok and Douglas Stuart (University of Texas, USA)

11:30 am--Applying Mechanical Theorem Provers

"ACL2: An Industrial Strength Version of Nqthm"

Matt Kaufmann and J Strother Moore (Computational Logic, Inc., USA)

"Comparing Verification Systems: Interactive Consistency in ACL2"

William D. Young (Computational Logic, Inc., USA)

"Mechanical Verification of Object Code Against Source Code"

Sakthi Subramanian and Jeffery V. Cook (Trusted Information Systems, USA)

2 pm--Practical Applications of Formal Methods

"Industrial Usage of Formal Development Methods:

The VSE-Tool Applied in Pilot Projects"

Frank Koob, Markus Ullmann, and Stefan Wittmann

(Bundesamt fuer Sicherheit in der Informationstechnik, Germany)

"Specifying, Validating and Testing a Semaphore System
in the TRIO Environment"

Angelo Gargantini, Lilia Liberati, Angelo Morzenti (Politecnico di Milano), and Cristiano Zacchetti (ATM-Azienda Trasporti Municipale, Italy)

"Feasibility of Model Checking Software Requirements"

Tirumale Sreemani and Joanne M. Atlee (University of Waterloo, Canada)

4 pm--Panel: From Theory to Practice---Bridging the Gap
Chair -- John Rushby (SRI Intern., USA)

Thursday, June 20

9 am--Keynote Talk

"Ontario Hydro's Experience with New Methods for Engineering Safety-Critical

Software", Mike Viola (Ontario Hydro, Canada)

10am--Program Verification

"Developing a Translator from C Programs to Data Flow Graphs Using RAISE"

Anne Elizabeth Haxthausen (Technical University of Denmark, Denmark)

"Verification of Consistency between Concurrent Program Designs and their Requirements"

Marsha Chechik and John Gannon (University of Maryland, USA)

11:30 am--Formal Specification and Verification II

"Verifying SOS Specifications"

Bard Bloom, Allan Cheng, and Ashvin Dsouza (Cornell University)

"A Correctness Proof of a Cache Coherence Protocol"

Amy Felty and Frank Stomp (Bell Laboratories, USA)

"The Specification of an Asynchronous Router"

Faron Moller (Kungl Tekniska Hogskolan, Sweden)

2 pm--Software Safety

"Safety Analysis Tools for Requirements Specifications"

Vivek Ratan, Kurt Partridge, Jon Reese, and Nancy Leveson (Univ. of Wash., USA)

"Impact and the Design of the Human-Machine Interface"

A. M. Dearden and M. D. Harrison (University of York, UK)

"Object-Oriented - No Panacea for Safety"

Reginald Meeson (Institute for Defense Analyses, USA)

4 pm--Panel on High Assurance Computing

Chair -- Richard Gerber (University of Maryland, USA)

6:30 Banquet

Guest Speaker: Nancy Leveson (University of Washington, USA)

Friday, June 21

9 am--Computer Security

"An Empirical Model of the Security Intrusion Process"
Erland Jonsson and Tomas Olovsson (Chalmers University of Technology, Sweden)

"Increasing Assurance Through Literate Programming Techniques"
Andrew Moore (Naval Research Laboratory) and
Charles Payne (Secure Computing Corp., USA)

"A Framework for Composition"
Todd Fine (Secure Computing Corporation)

"Composition of a secure system based on trusted components"
Ulf Lindqvist, Tomas Olovsson, Erland Jonsson
(Chalmers University of Technology, Sweden)

11:30 am--Testing

"Detecting Equivalent Mutants and the Possible Path Problem"
A. Jefferson Offut (George Mason University) and Jie Pan (PRC, Inc., USA)

"T-VEC: A Tool for Developing Critical Systems"
Mark R. Blackburn (Software Productivity Consortium) and
Robert D. Busser (Motorola, USA)

"Defining an Adaptive Software Security Metric From a Dynamic Software Fault -Tolerance Measure"
J. Voas, A. Ghosh, G. McGraw, F. Charron (Reliable Software Technologies) and
K. Miller (University of Illinois Springfield, USA)

1 pm--Conference ends [Breaks, lunches omitted above. PGN]

TOOLS FAIR

8 am--5:30 pm on Wed. and Thurs., 8 am--11:30 pm on Fri.
See demonstrations of NRL's requirements toolset SCR*,
CLInc's ACL2 theorem prover, two model checkers, and more...

FOR MORE INFORMATION, VIST OUR WEB SITE at
<http://www.itd.nrl.navy.mil/conf/compass96> or contact
Karen Ferraiolo, General Chair (ferraiolo@md.arca.com)
Stuart Faulk, Program Cochair (faulk@itd.nrl.navy.mil)
Connie Heitmeyer, Program Cochair (heimeyer@itd.nrl.navy.mil)

✦ The Second USENIX Workshop on Electronic Commerce: cfp

Bennet Yee <bsy@Play.UCSD.Edu>

Sat, 6 Apr 1996 14:58:35 -0800

See <URL:<http://www.usenix.org/ec.html>> for full details.
Or you can send e-mail to our mailserver at info@usenix.org.
Your message
should contain the line: send catalog. A catalog will be
returned to you.

Announcement and Call for Papers [abridged for RISKS]

The Second USENIX Workshop on Electronic Commerce
November 18-20, 1996, Claremont Hotel & Resort, Oakland, CA

Sponsored by the USENIX Association
Co-Sponsored by Fisher Center for Information Technology
Management, UC
Berkeley, and the School of Information Management and Systems,
UC Berkeley
Extended abstracts due: July 16, 1996

The Second USENIX Workshop on Electronic Commerce will provide a
major
opportunity for researchers, experimenters, and practitioners in
this

rapidly self-defining field to exchange ideas and present results of their work. This meeting will set the technical agenda for work in the area of Electronic Commerce by examining urgent questions, discovering directions in which answers might be pursued, and revealing cross-connections that otherwise might go unnoticed.

Doug Tygar (program chair)
Computer Science Dept, CMU
5000 Forbes Ave
Pittsburgh, PA 15213-3891
tygar@cs.cmu.edu
Fax: +1-412-268-5576



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 18: Issue 4

Monday 15 April 1996

Contents

- [OS/2 Warp TCP/IP misfeature](#)
[Pete Bentley](#)
- [Data entry omission extends prisoner's sentence](#)
[James K. Huggins](#)
- [Has the net reached a critical size?](#)
[Frederick Roeber](#)
- [Single names and identification](#)
[Colin Eric Johnson](#)
- [The joys of FAX machines](#)
[Drew Dean](#)
- [Real "Natural" language design isn't easy either](#)
[Peter Van Eynde](#)
- [Another Daylight Saving Time problem: Netscape 2.* reload](#)
[John F. Whitehead](#)
[Prentiss Riddle](#)
- [Another Daylight Savings Time risk: billing](#)
[Lorne Beaton](#)
- [Abuse of statistics about computer crime](#)
[Dan Barrett](#)
- [Phone-sex users on web index accidentally \[Name withheld by request\]](#)

- [Re: The weakest link](#)
[Paul Robinson](#)
 - [Re: X-Confirm-Reading-To: Pegasus woes ...](#)
[David Woolley](#)
[Peter Yamamoto](#)
 - [Re: A note on e-mail](#)
[David Milun](#)
[Jiri Baum](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✶ OS/2 Warp TCP/IP misfeature

Pete Bentley <pete@mimir.com>
Thu, 11 Apr 1996 12:44:22 +0100

[I was recently reminded of this one by a thread in a newsgroup I frequent]

It seems that in the OS/2 (2.1 and Warp) TCP/IP stack socket descriptors are system-wide. That is, they aren't per-process file descriptors, so if you can discover the number of some other process's socket (and `netstat -s` will helpfully list all the open sockets on the system) you can send `()`, `recv()`, `shutdown()` or do many other fun things with it.

Risks include the fact that anyone with telnet access to the machine (and OS/2 telnet security is a risk in itself) can write a program to subvert any TCP/IP server running on it.

A shame, because otherwise it's one of the better non-Unix implementations of the BSD socket API.

Pete

✂ Data entry omission extends prisoner's sentence

"James K. Huggins" <huggins@eecs.umich.edu>

Thu, 11 Apr 1996 10:30:12 -0400 (EDT)

Summarized from the *Detroit Free Press*, 11 April 1996, p. 4B.

John O'Valle was convicted in 1987 on charges of cocaine and weapons possession, and was expected to serve 20 years in prison. Later on, however, the sentencing judge reduced the sentence on technical grounds, making him eligible for release in 1992. The reduction was noted in O'Valle's written file, but not in the Department of Corrections' computer records. (Neither O'Valle nor his lawyer was notified of the change.)

In January 1996, prison officials reviewed his records and discovered the discrepancy. However, there is now a new problem. In 1995, O'Valle was convicted for possession of marijuana while in prison, a felony. Had he not been in prison at the time, he would have been guilty of a misdemeanor and not subject to jail time. So now O'Valle is serving time for a felony, which (presumably) never would have happened had he been released on time. State officials aren't sure what to do.

Officials aren't sure what happened. O'Valle's warden says that sentencing formulas are complicated, and the prison camp program and parole programs were in "transition" during the time O'Valle entered the system.

Perhaps a new story with an old moral: if you have replicated data sets, make sure that the data sets are consistent.

Jim Huggins, University of Michigan (huggins@umich.edu)

[The O'Valle course runs twistingly around. PGN]

✶ Has the net reached a critical size?

Frederick Roeber <roeber@iea.com>

Sun, 14 Apr 1996 22:15:20 GMT

I don't mean "critical" as in "film-at-eleven," but as in its size or penetration has reached a sufficient point for a process to occur.

In ten years on the net, I've only come across a couple other people with my last name. Websearches never revealed anything but links to my own data.

But within the past few weeks this has changed. RISKS had an article about www.switchboard.com, which lists some 350 Roebers. A new websearch finds a dozen Roebers. And suddenly the e-mail has started coming in-- "My name is <something> Roeber. Might we be related?" And this is all happening at once. It shouldn't be long before we have the whole family tree worked out.

I can't say there's a hard risk to this, other than the usual ones of privacy and how the net is making this an ever-smaller world. (But I do

hope none of those 350 www.switchboard.com hits are actually federal witnesses in the American witness protection plan. Pretty soon they'll stick out like sore thumbs.)

Frederick Roeber roeber@iea.com - roeber@cern.ch - roeber@caltech.edu

[Frederick has gone from being a Roeber Baron to being a DisRoeber, in short order. This must be where the Roeber meets the load. PGN]

⚡ Single names and identification

Colin Eric Johnson <colinj@unm.edu>
Mon, 15 Apr 1996 14:50:55 -0600 (MDT)

It seems that a friend's friend [name altered] decided that he wanted to only have a single name, Smith. When Smith had his name legally changed to just Smith one of the things that he had to do was get a new drivers license. So he headed on down to the local DMV.

It seems that the state of Oregon (at the time at least) had a computer system that required that both a first *AND* last name be entered for every persons license. Of course Smith only had one name (and the paper to prove it). So after struggling with the system for a while the diligent workers asked Smith to come back in a couple of days when they would have a license for him. And, sure enough, a couple of days later he returned to find a license with just the name Smith on it waiting for him, all

seemed to be
well.

While on a road trip, which Smith is prone to, he was pulled over for some sort of traffic violation. When he was offered up his license as per request the police officers were concerned with his lack of a second name (first or last? you decide). When they looked him up, he was not in Oregon at this time, they could not find any such person as "Smith" in the Oregon registry. At this point the police officers began to get suspicious. After much investigation, and a great deal of lost time and frustration on the part of Smith and the local constabulary, it was determined that the state of Oregon had done the following:

Failing to get the system to accept a single name for a drivers license they inserted a fictitious second name "Jay". They then simply altered the printing process so that only the name "Smith" actually appeared on the license. So to find Smith in the Oregon listing one would have to look under "Smith Jay".

The risks? Well, I believe trouble with the law would be obvious in this case. It might also cause problems in terms of employment where security and background checks are done as well as insurance. I believe that the least that could have been done would have been to explain to Smith what had been done to make this work. It might also be more appropriate to have a preset second name like "No Second Name" that could appear either in the list, on

the license or both.

Colin Johnson | colinj@unm.edu | <http://www.unm.edu/~colinj/>

✶ The joys of FAX machines

Drew Dean <ddean@CS.Princeton.EDU>

Sat, 13 Apr 1996 19:18:28 -0400

I was filling out an application for a summer job. Time was of the essence, so the company's normal employment application was FAXed to me. Printed in landscape mode, the bottom question, about whether I'd been convicted of a crime, got cut off by the FAX machine. Since various companies ask the question in different ways (some ask only about felonies, others include traffic citations, etc.), I decided that the best approach was to write in, "I have not been convicted of a felony" and to initial it. I then FAXed the application back.

I received a phone call within the hour asking if I was a felon. I had written the word "not" a little lower on the page, and it got cut off on the return trip. The situation was resolved, but somewhat amusing. I've fought laser printers that can't print closer than 1/4" to the edge of the page before, so I should have known about the problem, but I forgot.

RISKS: You think of FAX as being WYSIWYG, but it isn't quite. And you can't (easily) see what the recipient will get.

Drew Dean <ddean@cs.princeton.edu>
Department of Computer Science, Princeton University

✶ Real "Natural" language design isn't easy either

Peter Van Eynde <natst3@uia.ua.ac.be>
Thu, 11 Apr 1996 08:54:37 +0200 (MET DST)

The Netherlands and the Dutch-speaking region of Belgium have an organization to define the language (Dutch) spoken in the two counties. This organization reformed the Dutch language the last time in 1947-1954 by printing "Het groene boekje" (the little green book) Woordenlijst Nederlandse Taal. This book defines the rules and words used in the Dutch language.

In the last few years, there has been a feeling of unease with the spelling: it was felt that there were too many "illogical" words. So, a committee was formed to reform the language. But they proposed a radical change -- for example, the use of "c" sounding like "k" would be abolished. There was protest (and the grounding of a "We love the letter C" group) and the politicians told the committee to soften its proposal. It seems that they did this (in a very short time) by simply removing rules that were too radical, and then removing a bit more. (Nobody actually knows for sure: interviews with committee members result in a lot of finger pointing and "It works for me".)

So, version 2 came out, and is now law. It must be introduced in the schools, government and media. There is one snag: the rules are not "complete": the rules given don't even include the spelling of words given as examples, and there are cases without any rules.

Nobody uses the green book; people use dictionaries. But the major publishers found the rules and the words in argument, so introduced their own rules. Each publisher has different ones. Major newspapers also have an internal dictionary, and they did the same. One major encyclopedia publisher even found the new rules so bad that it refuses to use the new spelling.

The RISKS? I have to write my thesis *after* the new spelling becomes law, and I have to write it in Dutch. Now my only problem (and that of Microsoft, Lotus(oops IBM), Word-perfect (whoever owns them), etc), is *which* Dutch. This whole case is a textbook demonstration of the RISKS of language specifications and the influence of politics on "natural" or "logical" designs. 20.5 million people have to live with the consequences.

Peter Van Eynde [It's logic Jim, but not as we know it.]

⚡ Re: Daylight Savings Time problem: Netscape 2.* reload

"John F. Whitehead" <jfw@wral-tv.com>

Thu, 11 Apr 1996 18:45:14 -0400

There has been another side effect of the daylight savings time

change,
with the Netscape Navigator browser: caches have incorrect times
and no
longer work properly for documents that change frequently.

Netscape Navigator version 2.x for Windows and Unix platforms is
an hour off
in its cache-file handling. If a user tries to reload a page
that has
changed within the last hour, the browser still thinks its
cached version is
more up to date and won't retrieve the new version. (After an
hour, this is
no longer an issue.) This has been a problem with news
organizations (such
as ours), chat/bulletin boards, and java applets that need to be
updated
frequently.

Netscape's "force reload" procedure (shift key + reload button)
doesn't
always work either: the only solution is to flush the memory and
disk caches
before a reload, or to set them to size zero. Netscape has made
no official
statement, but apparently has said the bug won't be fixed in the
next
version of the software (2.1) but in the one after that (3.0
(Atlas)).

The Macintosh version does not suffer from this bug, nor do
versions 1.x, or
browsers from other manufacturer.

The risk (aside from the obvious one related to programming for
time
changes) is trusting that a market-leader software company is
going to have
bug-free software.

John F. Whitehead OnLine Technical Director
919-821-8605 jfw@wral-tv.com <http://www.wral-tv.com>

[This problem was also reported by CurtAkin@aol.com and
Prentiss Riddle <riddle@is.rice.edu> -- next message. PGN]

⚡ Another Daylight Saving Time problem: Netscape 2.* reload

Prentiss Riddle <riddle@is.rice.edu>

Mon, 15 Apr 1996 09:14:54 -0500 (CDT)

[...] One workaround is said to be to run Netscape in California
time, e.g.
under Unix:

```
setenv TZ PDT ; netscape &
```

Defying the RISKS tradition of intoning that "the risks are
obvious",
one could draw the following lessons:

- Time-dependent functions should be tested using multiple
time
zones and both DST- and non-DST dates.

- In networked applications, local time issues can cause
more than
just local problems.

Prentiss Riddle <riddle@rice.edu> <http://is.rice.edu/~riddle>
RiceInfo Administrator, Rice University

⚡ Another Daylight Savings Time risk: billing

Lorne Beaton <beaton1@server.uwindsor.ca>

Thu, 11 Apr 1996 16:20:49 -0400 (EDT)

My university recently (ca. January 1, after a testing period of
about a

month) instituted a new dialup service, for which students and faculty are charged 75 cents per hour peak and 60 cents off-peak. A couple of days ago I logged on and saw something like the following in my logon message:

```
> Charges THIS month to date    500 minutes for a cost of $
49.59
> Charges LAST month (total)    2089 minutes for a cost of $
24.76
```

(Note that these aren't the exact figures, but you get the idea.) Needless to say I was consternated. After complaining to the admins, I learned that the billing discrepancy arose from the change to Daylight time. Night owl that I am, I happened to be logged in at the exact moment that 2:00 a.m. EST became 3:00 a.m. EDT. Needless to say, this was the first time they had dealt with the changeover. Happily, the problem has since been fixed, but the risk is self-evident.

Lorne Beaton <beaton1@server.uwindsor.ca>

✶ Abuse of statistics about computer crime

<barrett@liberation.cs.umass.edu>
Fri, 12 Apr 1996 12:52:50 -0400

The March 1996 issue of IEEE COMPUTER contains an article on the rise of computer crime ("Security and Privacy TC," by Deborah Cooper and Charles Pfleeger, pp. 118-119; TC = Technical Committee). Based on a table of statistics obtained from the CERT Coordination Center, the

article claims that computer crime is undergoing a "dramatic escalation." Whether or not this is true, the article is seriously flawed, and it points out the risks of shoddy statistical reasoning.

Here is an excerpt from the table, which has the heading, "Computer Emergency Response Team (CERT) statistics show that computer attacks are on the rise."

YEAR	INCIDENTS REPORTED
1988	6
1989	132
1990	252
1991	406
1992	773
1993	1334
1994	2341

On first glance, this certainly appears to be a "dramatic escalation" in computer crime... or does it? Let's look at how much information was not presented in the article.

The table heading discusses "attacks," but the table column says "incidents." So what exactly is an "incident?" Is it a report of an alleged attack? (Likely, given that CERT is usually the recipient of unsolicited reports.) Or is it a verified attack, meaning that erroneous reports were somehow weeded out? If it was verified, how was it verified? The article doesn't say.

I wrote to Pfleeger with this question, and he responded that "the source of these statistics is CERT" and I would "have to contact them for

the interpretation of their data." In other words, Pfleeger, Cooper, and IEEE COMPUTER published a table of statistics that the authors did not not themselves understand. So I wrote to CERT, and their response indicated that an "incident" is a report, and that they "don't talk to law enforcement people at all" to verify that an attack is real "unless a site requests us to."

The abuse of statistics gets worse. While the number of incidents in the table is approximately doubling every year, so is the population of the Internet (source: The Economist, July 1995). In other words, the number of incidents grows linearly with the size of the population, which is completely unsurprising. This fact is not mentioned anywhere in the article. Pfleeger argued (by email) that "technical and physical security controls" have improved since 1988, and yet incidents have continued to increase "in spite of improved protection." That is an interesting hypothesis but hardly a reason to ignore the growth of the Net as a possible source of increased reports. The CERT representative reported that she didn't "know why the authors of the article didn't mention the relationship between the number of incidents and the number of Internet users."

Similarly, the visibility of CERT has grown greatly since 1988, and this could account for an increase in reported incidents. Again, this is not mentioned in the article. Both Pfleeger and CERT say that

measuring CERT's visibility is a non-trivial task, and I agree. Still, the effect should have at least been mentioned in the article.

Footnote 1 of the table mentions that "some incidents have ongoing activity for long periods of time (i.e., more than a year)." I asked Pfleeger whether "ongoing activity" meant "ongoing penetration of a compromised system," or "ongoing interaction with CERT," since the phrase is ambiguous.

Pfleeger DIDN'T KNOW and suggested I ask CERT. He also didn't know whether the phrase "some incidents" referred to a majority or a (possibly insignificant) minority. By highlighting the incidents with long ongoing activity, the table takes on a negative slant. After all, one could just as easily have focused on the opposite, saying that "some incidents lasted only a few minutes."

My intuition and experience tell me that security incidents are indeed increasing. In other words, I believe the basic premise of the article.

Nevertheless, the article's reasoning is flawed and contributes only to the prevalent misinformation about computer crime and security.

Dan Barrett dbarrett@ora.com <http://www.ora.com/item/bandits.html>

Author, "Bandits on the Information Superhighway" (O'Reilly & Associates)

⚡ Phone-sex users on web index accidentally

<[Name withheld by request]>

Wed, 10 Apr 96

To see if any of my personal WWW home pages have been indexed by web crawlers, I sometimes query the popular web search engines with my first and last names. Imagine my surprise when, amid the usual links, I found several that referred to caller-id files!

Upon visiting the links, I discovered many text files containing a column of phone numbers and a matching column of people's names. The files were broken up by month and year, and contained hundreds of listings each. Some of the names in the list were 'Pay Phone' and 'City of XXX' and 'State of XXX'. Often, a name and number would be repeated several times in a row, presumably denoting multiple calls from one number.

When I removed all but the fully qualified host name from the URL address, I was presented with the first HTML document that I'd found on this server. It was functional, yet spartan: clearly intended for the page-developer's use only. From it, I ascertained that the phone lines from which the caller-id's were taken were all named after different kinds of sexual activity.

Forgive me for jumping to conclusions, but I believe that these files were created by a phone-sex service. Perhaps they are used to identify satisfied customers, or to help direct incoming calls to the proper 'talent'.

The RISKS: too many! First, it is foolish to allow proprietary information

be stored on a server connected to the internet. Second, any time that you dial the phone, unless you're calling from a Pay Phone or the State of XXX, the marketeers at the other end probably know who you are. Finally, free access to demographic data may be hazardous to your marriage, or job, or whatever.

⚡ Re: The weakest link (Reifschneider, [RISKS-18.02](#))

<ROBINSON_PAUL@Tandem.COM>

15 Apr 96 09:49:00 -0700

Sean Reifschneider reports that Social Security Administration employees sold SSNs and "mother's maiden name" info to a credit-card fraud ring. Many credit card issuers require "activation" of newly-issued cards, i.e. the recipient must call a toll-free number and give this kind of "identifying" information before they can use the new card.

Actually, the weakest link is "the clerk who's paid \$12K/year" at the credit-card issuer. Recently I received a new card, called the number, and adamantly refused to give my SSN over the phone. The somewhat flustered clerk eventually activated my new card, having received only the credit-card number and the zipcode (postal code) printed on the accompanying letter. No SSN, no "mother's maiden name," NOTHING else.

If all I need is the card and the letter, why pay off SSA employees?

I have written to the credit-card issuer, no response yet.

--paulr

⚡ Re: X-Confirm-Reading-To: Pegasus woes ... (Yamamoto, [R 1802](#))

David Woolley <david@djwhome.demon.co.uk>

Sun, 14 Apr 96 12:58 BST

>The "problem" is due to a new release of Pegasus which added a directed
>confirmation header field as well as keeping the old
confirmation header

The new header was added precisely because the old version was causing
problems with mailing list, but people have to upgrade the
reading version
not the sending version to gain the full benefit.

However, this whole thing shows the common risk that users will demand
certain features of a product ("read" receipts are a very popular feature
of Pegasus) without realising the full implications (namely they will get
a reply from every Pegasus user on the mailing list, and possibly compromise
the privacy of those subscribers).

There is, however, a very simple solution for MajorDomo and probably for
listserv, just filter out the offending headers. The standard MajorDomo
already filters out Return-Receipt-To:, a rather more common, non-standard
header, with similar effects. Adding such filters to MajorDomo is a

reasonable local customisation.

Although there are now safe standards for achieving these results, which shouldn't propagate through a properly configured list server, it will be many years, if ever (commercial factors, rather than good technical design are now controlling the e-mail market), before they are widely implemented, and more ad hoc methods of meeting the market demand for this feature will arrive first.

[✶ X-Confirm-Reading-To: Pegasus woes ... \(Yamamoto, RISKS-18.02\)](#)

Peter Yamamoto <pjyamamo@daisy.uwaterloo.ca>
Wed, 27 Mar 1996 00:47:51 -0500 (EST)

Two things about automatic e-mail confirmation, although the risk is nothing new to RISKS readers...

Recently, on a mailing list I maintain, a Pegasus (the name of a Mac/Windows e-mail reader) user posted a message with a line:

```
> X-Confirm-Reading-To: <e-mail address>
```

This would be fine if Pegasus respected the field value when acting on the presence of this field. But Pegasus programmers apparently took the RISK of assuming that they didn't have to. Now every list member using Pegasus is generating a confirmation message to the list.

Peter Yamamoto University of Waterloo Waterloo, Ontario,

Canada N2L 3G1

519-888-4567 x3299 PJYamamoto@UWaterloo.CA <http://daisy.uwaterloo.ca/~pjyamamo/>

✉ Re: A note on e-mail ()

Davin Milun <milun@cs.Buffalo.EDU>

Fri, 12 Apr 1996 10:46:24 -0400 (EDT)

While I tend to disagree with your preference for "e-mail" over "email", that pales in comparison for my dislike of the use of "email" as other than a mass noun.

Sentences like "send me an email" or "I received an email today" bother me intensely. "Mail" is a mass noun --- no native English speaker would replace "an email" with "a mail" in the above sentences! But many casually do it with "email", even though "email" is just "electronic mail".

Listen everyone, it's "send me some email" or "send me an email message" or "send me a piece of email" etc..

(So, maybe PGN is correct after all. Maybe we do need the hyphen to remind people that "e-mail"/"email" is a modification of "mail".)

Davin Milun milun@cs.Buffalo.EDU <http://www.cs.buffalo.edu/~milun/>

Cory Search - Aquaria index: <http://aquaria.cs.buffalo.edu/>

[And PGN left all of Davin's "email"s intact. Am I ("Am I" = the French pronunciation for "email", sort of) Nice?]

✉ Re: Notes on e-mail (Sandee 18.01, Stolz 18.02)

Jiri Baum <jiri@baum.com.au>

Sun, 14 Apr 1996 09:07:01 GMT

```
>> [...] "co=F6perate", "na=EFf", and "Bront=EB.". [...] ...
>> Usenet (at least NNTP) is generally 8-bit transparent, and
any European
>> soc.culture group will tell you that ISO 8859-1 usually works
[...]
```

Nothing is so simple as it seems at first sight.

There is not only ISO 8859-1, but also ISO 8859-2, ISO 8859-3 etc. For a practical example of the difficulties, see soc.culture.esperanto. (Esperanto has the endearing feature that stripping supersigns tends to cause a lot more confusion than in say Czech.) Most people there have given up and are using the ugly method of a trailing x (which is human-readable yet machine-tractable).

[...]

Using multipart/mixed and separate charsets for each section? While that would be acceptable to people who have MIME, it would add to the bulk of the headers that one has to skip in a plain text reader.

Of course, that's assuming that each contributor only posts in one charset. Multi-charset contributions would be worse still... I guess it'll be a long time before I can put my name on my Esperanto postings properly (the r

should be \sqrt{r} , and the i should be \sqrt{i} .

Jiri Baum



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 18: Issue 5

Friday 19 April 1996

Contents

- [NYPD phone system cracked](#)
[Fernando Pereira](#)
- [Judge: Computer encryption codes ruled protected speech](#)
[Jay J. Kahn](#)
- [Euthanasia via computer](#)
[Pete Grooby](#)
- [Internal Revenue Service browser](#)
[Dave Del Torto](#)
- [Capitalizing on the Millennium](#)
[Steve Summit](#)
- [Consumer risks on the Internet](#)
[Mike Wyman](#)
- [Re: The joys of FAX \[and other\] machines](#)
[Greg Gomberg](#)
- [Re: Daylight Savings Time problem: Netscape 2.*](#)
[Mark Phaedrus](#)
- [Re: OS/2 TCP/IP security](#)
[Lionel B. Dyck](#)
- [Re Microsoft Exchange e-mail aliases etc.](#)
[Chris Koenigsberg](#)

- [More Microsoft Viruses](#)
[Edupage](#)
 - [Demise of the Web Predicted](#)
[Edupage](#)
 - [Web Called "Ultimate Act of Intellectual Colonialism"](#)
[Edupage](#)
 - [The RISKS of College Admissions](#)
[Maddi Sojourner](#)
 - [IEEE Symposium on Security and Privacy 1996](#)
[Dale M. Johnson](#)
 - [Safety Critical Systems Vacation School Announcement](#)
[Mike Brown](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ NYPD phone system cracked

Fernando Pereira <pereira@research.att.com>

Fri, 19 Apr 1996 11:06:00 -0400

The AP reports today that, according to the **New York Post**, callers to New York Police Department headquarters for 12 hours ending 6am Tuesday [16 Apr 1996] heard a bogus recording that included the following: ``You have reached the New York City Police Department. For any real emergencies, dial 119. Anyone else -- we're a little busy right now eating some donuts and having coffee.''

It continued ``You can just hold the line. We'll get back to you. We're a little slow, if you know what I mean. Thank you.''

The NYPD had no immediate comment, but unnamed police sources believe hackers broke access controls and changed the message.

Fernando Pereira, 2B-441, AT&T Bell Laboratories

600 Mountain Ave, Murray Hill, NJ 07974-0636 pereira@research.att.com

[Also reported by Steven Bellovin <smb@research.att.com>. PGN]

⚡ Judge: Computer encryption codes ruled protected speech

Jay J. Kahn <jkahn@smiley.mitre.org>

Wed, 17 Apr 1996 10:49:58 -0500

Source: <http://www.usatoday.com/news/nds19.htm> [PGN Abstracting]

U.S. District Judge Marilyn Hall Patel released a ruling on 16 Apr 1996 that mathematician Daniel Bernstein could try to prove that the U.S. export controls on encryption technology are too broad and violate his right to communicate with other scientists and computer buffs -- a right protected by freedom of speech. (Bernstein's cryptographic programs are called Snuffle and Unsnuffle. The U.S. State Department decided in 1993 that Bernstein's written article and programs required export licenses [because purveyors are considered as being international arms dealers under ITAR], but later backed down on restricting the article; Bernstein then had sued for release of the programs.)

David Banisar of the Electronic Privacy Information Center (EPIC) is quoted in the news item: ``It's important to recognize that computerized information has the same kind of legal protection that printed information has.''

[There are various news items on 18 Apr in the press. The EFF EFFector Online 09.04 (see <http://www.eff.org>) provides useful background. PGN]

✶ Euthanasia via computer

Pete Grooby <Peter_Grooby@trimble.co.nz>
Fri, 19 Apr 96 09:57:40

I saw a news item last night about a euthanasia law which will soon be passed in the Northern Territory of Australia. During the article they showed the system by which patients could terminate their own lives.

An automated syringe full of a lethal substance was hooked up to a laptop. The patient was asked a series of questions about whether or not they really wanted to kill themselves. At the end of the questions they click on a button to activate the injection and they die within 30 seconds afterwards.

This would seem to be the ultimate in mission-critical applications, and one assumes that it has been tested thoroughly (with out anyone attached).

I also noted that the laptop was a Mac. I shudder to think of the risks of running such a system under Windows 3.1.

Pete Grooby

[This is in today's papers here. It would be difficult to do

a complete

system test without a real person; all the components might work just fine

individually without being properly integrated. Worse yet would be having

a specification that is concerned only with the system functioning

correctly when the final YES confirmation is input, without worrying about

accidental triggering, false positives, sneak paths, hazards, race

conditions, malicious reprogramming to change the defaults or even

have the program masquerade as a common icon such as file-delete instead

of person-delete that might trap unsuspecting victims who happened to use

the laptop, etc. No jokes about poisoned apples, please. PGN]



Dave Del Torto <ddt@lsd.com>

Tue, 16 Apr 1996 04:40:51 -0700

Subject: Internal Revenue Service browser

[from SF Examiner somewhere around 12-14 April 96]

"IRS Worker Took Peek at Celebrities' Records" [Associated Press]

Memphis - A former IRS employee who said boredom had led him to peek at

the tax records of President Clinton, Elvis Presley, and other famous

people has been acquitted of federal charges. Robert Patterson, 38, said

it wasn't malicious - he was just trying to learn how to better use the

Internal Revenue Service computers. "I was sitting there bored, so I

started punching up names," said Patterson.

Hmmm. We do it, it's "malicious cracking/hacking" and they toss us in the clink... they do it, and it's "practice" (and they get acquitted).

And these are the people who want to escrow my keys? As IF!

Not only that, but also if the guy's so damn bored, why doesn't he spend some time FIXING the damn computer systems at IRS (see current cover of Information Week mag). Not that I particularly WANT them to fix the infernal revenue suckers...

BTW, where do they find these people? He's hacking around in Clinton's tax records and he doesn't expect Secret Service agents crawling up his yin-yang within minutes? Obviously, "thinking too much" is not this chap's problem.

✶ Capitalizing on the Millennium

Steve Summit <scs@eskimo.com>

Thu, 18 Apr 1996 14:10:12 -0700 (PDT)

I was intrigued by the subject of an article in the **Seattle Times** business section, 17 Apr 1996, which needs no further comment for RISKS readers:

[by Greg Heberlein, Seattle Times business reporter]

A Bellevue company's stock has tripled in value in the past 12 trading sessions...

Data Dimensions is a service company whose sole mission --

since 1993 -- has been to help companies reconfigure their computers so the years 2000 and beyond will not be recognized as 1900s. There is believed to be a multimillion-dollar market for such a service.

And then, yesterday evening, I noticed a new book in the computer section of my local technical bookstore:

Jerome T. Murray and Marilyn J. Murray
The Year 2000 Computing Crisis
A Millennium Date Conversion Plan
McGraw Hill, 1996
ISBN 0-07-912945-5

It was full of suggested code for patching legacy systems.

Steve Summit scs@eskimo.com

[How many more such companies will go public before 1/1/00?
And what will they do for their stockholders thereafter? PGN]

⚡ Consumer risks on the Internet

Mike Wyman <wyman@tiac.net>
Thu, 18 Apr 1996 21:11:57 -0400

The most publicized risk associated with consumer commerce on the Internet is that of one's credit card number being misappropriated. This risk pales beside the one recently introduced by PC Flowers and Gifts, a joint venture involving no-one less than IBM.

I attempted to use PC Flowers (<http://www.pcgifts.ibm.com>) to order (a fairly extravagant) floral arrangement to celebrate my mother's 75th

birthday. To my chagrin (and embarrassment) the flowers never arrived. After
two e-mail messages over three days inquiring as to the state of my
(ostensibly) confirmed order, I received the following response:

>Dear Mr. Wyman,

>

>Please accept our apology for the delay in messaging you back.

>

>PC Flowers & Gifts recently moved our web site servers and we have been

>experiencing some problems. Unfortunately, we did not receive order number

>100061. Since we have no record of the order, your credit card was never

>charged. Our programmers are working on this matter and hopefully very soon

>the problem will be corrected.

>

>We are very sorry for any inconvenience this has caused.

Belinda @ PC

>Flowers & Gifts

>

I would have much preferred having my credit card stolen than having to explain to my mom why she did not receive a gift on her 75th birthday.

Obviously, these folks leave a little bit to be desired when it comes to testing the installation of new systems.

Mike Wyman wyman@tiac.net <http://www.tiac.net/users/wyman/>

✉ Re: The joys of FAX [and other] machines (Dean, [RISKS-18.04](#))

Gomberg Greg <GombergG@logica.com>

Tue, 16 Apr 96 10:35:00 bst

I expect you'll get a fair bit of "me too" follow up to Drew Dean's item on margin losses in [RISKS-18.04](#) on the "joys of FAX machines". Here's mine.

I have seen a lot of this sort of thing from attempts to pass documents between US and European offices. Because of the difference in paper sizes we lose material from margins on the long edge (US->European) or the short edge (European->US). The differences are small and the affected areas are usually blank, but occasionally ...

I wish this were specific to FAX machines; it affects photocopying and, most irritating, documents published as Postscript - these are cropped by the printer. The latter is most irritating because it is easily avoided by the "publisher" and difficult for the recipient to fix (or even to notice). Even documents sent as word processor or markup files are not immune because the printed versions do not correspond - readers thinking they have identical documents can be confused and, in bad cases, cross references are incorrect.

Greg Gomberg [Greg's disclaimer covered by RISKS standard disclaimer]

✉ Re: Daylight Savings Time problem: Netscape 2.* (Whitehead, [R 18 04](#))

Mark Phaedrus <phaedrus@halcyon.com>

Tue, 16 Apr 1996 10:23:50 -0700

Actually, Netscape has publically announced that "We are preparing to release Netscape Navigator 2.02 in the next two weeks to fix this problem."
(Source: <URL:http://home.netscape.com/misc/DST_err.html>.)
They also give one other, rather unsatisfactory workaround (besides clearing or zeroing your disk cache, or setting the time-zone variable correctly): set your machine's clock back an hour...

[Also noted by
Prentiss Riddle <riddle@is.rice.edu> and
"J. David Stanton, Jr." <jstanton@coin.state.pa.us>. PGN]

✶ Re: OS/2 TCP/IP security (Bentley, [RISKS-18.04](#))

Talklink OS/2 BBS <rrs0066@ibm.net (Lionel B. Dyck, OS/2 Advisor)>
16 Apr 1996 17:56:58 EDT

I just read [RISKS-18.04](#) and found the piece on OS/2's TCP/IP Telnet security worthwhile but somewhat outdated. IBM provides the user the ability to replace the existing (default) Telnet Login.exe with another (loginunx.exe) that supports multiple userids with unique passwords that are maintained in a file that is encrypted. The password file (PASSWD) is maintained in the same manner as the Unix password file - unfortunately IBM doesn't supply a tool to manage this file but you can ftp from various OS/2 ftp sites a file called PASSWD.ZIP which provides a tool to maintain that file. Thus the OS/2

user who enables Telnet to their workstation can provide a reasonably secure interface to only trusted users.

Lionel B. Dyck, OS/2 Advisor (Talklink OS/2 BBS)
syslbd@ncal.kaiperm.org

✈ **Re: Microsoft Exchange e-mail aliases etc. ([RISKS-18.02](#))**

Chris Koenigsberg, ckk@pobox.com <ckk@uchicago.edu>

Tue, 16 Apr 1996 20:39:59 GMT

Following up on the discussion begun in 18.02, here's another relevant incident involving bad aliases (I think it was Microsoft Mail rather than Exchange):

Just a few days ago, we suddenly started getting obviously internal, confidential e-mail, from various members of some local law firm, addressed to our Mailer-Daemon (which is forwarded to 3 responsible sysadmins here).

Repeated replies from me to the senders, warning them to stop including our Mailer-Daemon in their internal replies, were unheeded. Finally, a day later, I got a frantic phone call from one of them, who was taking on the added volunteer duty of administering the Microsoft Mail system there. He said that his colleagues were all asking what the hell was going on, why was I replying to their internal confidential mail messages that they were simply addressing to "All-Staff"?

Somehow he had literally added our Mailer-Daemon to an internal system-wide MS-Mail "All-Staff" alias there. I assume that he, or someone else, had previously tried to e-mail someone here, perhaps in our Law School, had made a typo in the address, gotten a reply back from the infamous Mailer-Daemon, and mistakenly pasted the Mailer-Daemon's address into their PERSONAL alias book, and subsequently copied their PERSONAL aliases blindly into the SYSTEM alias. (did I ever tell you about the fascinating love letters we get, mistakenly addressed to the Mailer-Daemon? :-)

Their internal MS-Mail users would simply address their messages to "All-Staff" and not even see the expansion of the alias, which is reasonable (why should the users be bothered with the expansion for every message to the whole staff?).

(in fact, the first of their puzzling messages leaked to us was from this guy, saying "OK everyone, I've finally got the staff-wide alias working! Fire away!" :-)

The problem is, no one was carefully auditing the results. Since no one actually was paid to be a system administrator, no one bothered to carefully examine the system-wide aliases. So their confidential mail, about alternative possible strategies of argument before the judge in a current pending case, were all forwarded to us!

Of course we offered to delete our copies for a very reasonable fee :-) :-) (no, I'm kidding, we really did delete them, although perhaps

they made it onto a backup tape or two, maybe even a long-term archival storage tape? hmm...)

Chris Koenigsberg ckk@uchicago.edu, ckk@pobox.com
<http://www2.uchicago.edu/ns-ac/ckk/index.html> (also <http://www.pobox.com/~ckk>)

⚡ More Microsoft Viruses (Edupage, 16 Apr 1996)

Edupage Editors <educom@elanor.oit.unc.edu>
Tue, 16 Apr 1996 17:10:07 -0400 (EDT)

First there was the Word virus -- now there's a Word Prank Macro Virus, located in a document on ActiveVRML, Microsoft's software tool for developing 3-D Web sites. But what's worse, is that Microsoft had to inform the programmers who attended its Professional Developers Conference last month that one of the CD-ROMs it distributed was infected. A cure is posted on Microsoft's Web site < <http://www.microsoft.com/> > (*Investor's Business Daily*, 15 Apr 1996, A8)

⚡ Demise of the Web Predicted (Edupage, 16 Apr 1996)

Edupage Editors <educom@elanor.oit.unc.edu>
Tue, 16 Apr 1996 17:10:07 -0400 (EDT)

Mark Stahlman, president of New Media Associates, predicts the death of the Web this year: "Advertisers will dump the Web, and businesses that depend on ad support will become uneconomic. But the cause won't be

the poor performance caused by 'clogged pipes';... it's more fundamental. The Web is a terrible place to manipulate people's unconscious fears, which is the aim of consumer advertising... Advertising on the Web has to be information, not manipulation. This is because the medium doesn't permit the psychological games that 'impact' a modern audience.... unless the Web becomes television, as @Home and others hope. If the Web could readily deliver video-server-based moving images, then the manipulative techniques of TV ads could also be Web-delivered. But the bandwidth just isn't available, and probably won't be for as long as 10 years... But there's still a chance something quite new could happen. The Web is a medium for information and education -- not unconscious mental manipulation. What if the Web's real capability is taken seriously and it becomes the world's largest adult education system?" (*Information Week*, 8 Apr 1996, p. 100)

✶ Web Called "Ultimate Act of Intellectual Colonialism" (16 Apr 1996)

Edupage Editors <educom@elanor.oit.unc.edu>
Tue, 16 Apr 1996 17:10:07 -0400 (EDT)

Anatoly Voronov, the director of Glasnet, an Internet service provider in Russia, says: "It is just incredible when I hear people talking about how open the Web is. It is the ultimate act of intellectual colonialism. The

product comes from America so we either must adapt to English or stop using it. That is the right of any business. But if you're talking about a technology that is supposed to open the world to hundreds of millions of people you are joking. This just makes the world into new sorts of haves and have nots." (*The New York Times*, 14 Apr 1996, Sec.4 p1; in Edupage)

✶ The RISKS of College Admissions

Maddi Sojourner <maddi@genmagic.com>

Wed, 17 Apr 1996 13:57:58 +0000

It's April, which brings us Daylight Savings Time, tax returns, and big, fat envelopes (or small, thin ones). Now is the time that high-school seniors [SEE NOTE 1, below] around the U.S. get responses from the college of their choice and discover whether the feeling was mutual.

I am an alumna of a university that depends on volunteers to contact and interview the applicants. Let's call it Eastern Elitist University (EEU) [SEE NOTE 2, below], as it is very selective (11%) and expensive. The interviews are useful for the students, who have questions about the school or the admissions process, and to the admissions office, which gets a personal assessment of the candidate. The process is particularly important for candidates who live too far away to schedule a visit to EEU (those willing to travel usually do so after getting acceptances).

Anyway, I have interviewed a few candidates a year for several years. This year, the person in charge of my geographic area, Silicon Valley/South Bay, handled a lot of the communications by e-mail for those of us who had access. All important communications were also sent by US Postal Service. On Monday, April 8, I received an e-mail message with a list of admitted candidates, and one of them was a student I had interviewed. We were instructed to contact our admits no earlier than Tuesday at 5 PM (to allow for the accept/reject letter to have arrived first). We were supposed to encourage "our" candidates to attend local receptions, visit EEU, and we were to answer any additional questions, with the goal of encouraging them to accept the admission offer.

On Tuesday, April 9, I contacted the student, whom I will call "Walter Williams." I introduced myself and congratulated him on admission. It turned out that Walter had already received another call from someone else who read the e-mail message, so he was not surprised to hear from me. But there was a problem: Walter had received a rejection letter from EEU.

A call to the South Bay chair unearthed where the process went awry: EEU sent a printout, via Federal Express, of the area's admitted students to the Northern California chair. He communicated these results to each regional chair by telephone. Each of the regional folks had to contact the interviewers.

One of the admitted students, who went to the same high school as Walter Williams, was named "Warner Wilkins." And somehow, both Warner and Walter got on the South Bay chair's list. Since the e-mail message had all the information nicely formatted (candidate, high school, interviewer, status, etc.), it made the information look official. But it wasn't transmitted that way. And how did Walter get on the list? Well, either Mr. Northern California said the wrong name, or Mr. Silicon Valley heard it. [See NOTE 3, below.]

But I'd hate to be at the Walter Williams household that evening, dealing with the rejection letter, two acceptance phone calls, and finally, two abject apologies (from myself and Mr. Silicon Valley).

The RISKS? What seemed like a modern, efficient way to distribute information was really an old-fashioned game of telephone. EEU sent the data out as hard-copy, and the results were distributed as each level saw fit. The twist on this old problem was the high-tech delivery at the final link. If the whole process had been electronic, then the human error of confusing "Walter Williams" and "Warner Wilkins" would not have occurred. But we can't go all-electronic until all the volunteers are willing to, and that's how we ended up with this "hybrid" data.

[NOTE 1: hyphenation (not hypenation!) by PGN, who did not want to encourage those school seniors who are high all the time.

NOTE 2: Eli-tist? That might just refer to Yale and its

namesake!

NOTE 3: In California, chili con carne might become Siliconcarny! PGN]

IEEE Symposium on Security and Privacy 1996

"Dale M. Johnson" <dmj@linus.mitre.org>

Thu, 18 Apr 1996 09:00:12 -0400

Current topics on risks and computer security will be covered at the upcoming IEEE Symposium on Security and Privacy to be held 6-8 May 1996 at the Claremont Resort in Oakland, California. Since 1980, the Symposium on Security and Privacy has been the premier forum for presenting developments in computer security and for bringing together researchers and practitioners in the field. This year topics will range from security flaws in Java and HotJava, presented by Drew Dean, Ed Felten, and Dan S. Wallach from Princeton University, to covert channels and to security standards for the OMG's CORBA. The discussions should be very interesting. For further information see <http://www.cs.pdx.edu/SP96/> or contact me at dmj@mitre.org.

Dale Johnson, Chair

Safety Critical Systems Vacation School Announcement

Mike Brown <mjdb@dorevale.demon.co.uk>

Wed, 17 Apr 1996 16:49:37 GMT

THE INSTITUTION OF ELECTRICAL ENGINEERS
Savoy Place London WC2R 0BL
The Fifth Vacation School on Safety Critical Systems
Robinson College Cambridge 15 - 18 September 1996
(Co-sponsored by the British Computer Society)

Since 1992 the Institution of Electrical Engineers has organised an annual vacation school aimed at providing participants with a broad understanding of the principles of safety critical systems engineering, with particular emphasis on the theory and practice of current techniques for defining and managing the risk potential of computer-based systems. The fifth in this series of intensive short residential courses will be held this year at Robinson College, Cambridge, from Sunday 15th September until Wednesday 18th September.

The field of safety critical systems includes those processes, products, and services where a breakdown or design fault is likely to result in death or injury or damage to property. Added emphasis is given to the problem of protecting against such consequences by the development of new legal codes of product liability. It is likely to become increasingly difficult for companies that have not employed explicit risk minimization and management techniques to argue successfully that they have exercised proper legal care for the safety of their products and services.

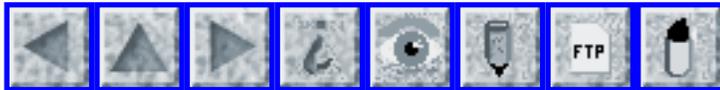
The structure of the vacation school is designed to provide a comprehensive survey of the issues involved in safety critical systems engineering at a

professional but non-specialist level. The goal is to provide a framework of common understanding to link people working in the requirements capture, architectural design, risk and hazard assessment, reliability, software, quality assurance, human factors, and project management functions; and to provide a good foundation for their future professional development.

The vacation school lecture programme is based on the "safety lifecycle" concept embodied in International Standard IEC 1508, (Functional Safety of Safety-Related Systems), supplemented by a closely coordinated case study to provide learning reinforcement and a thematic linkage between the lecture sessions.

For full details of the vacation school programme and a registration form, please send e-mail to SEvans@iee.org.uk or write to Miss Sarah Evans at the address given at the head of this announcement.

Mike (M J D Brown: Newhaven, Peterchurch, Herefordshire HR2 0RT, England)



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 18: Issue 6

Tuesday 23 April 1996

Contents

- [Java security/privacy bug](#)
[Daniel Abplanalp and Stephan Goldstein](#)
- [Swedish court fines parents for son's overly long name](#)
[Li Gong](#)
- [Baltimore Throws the Book at Criminals](#)
[Peter Wayner](#)
- [AMD5K86 Floating-Point Division Algorithm](#)
[J Strother Moore](#)
- [MCI recommending bad security practices](#)
[Chad Ray McDaniel](#)
- [Sometimes, stratum 1 time isn't so good](#)
[Dave Hsu](#)
- [Filename bug in Windows 95](#)
[Vsevolod Ilyushchenko](#)
- [Web page e-mail addresses Risky](#)
[Ray Normandeau](#)
- [Re: Web Called "Ultimate Act of Intellectual Colonialism"](#)
[Vadim Antonov](#)
[A. E. Siegman](#)
- [Re: Euthanasia via computer](#)

[Paul Menon](#)

- [Yes, there are new Word Macro viruses, no, this isn't one of them](#)

[Rob Slade](#)

- [888 Risks](#)

[Russ Broomell](#)

- [Databases without SSNs and UIDs?](#)

[Robert Ellis Smith](#)

- [Info on RISKS \(comp.risks\)](#)
-

✶ **Java security/privacy bug**

TERMINATOR <goldstei@iamexwi.unibe.ch>

Mon, 22 Apr 96 17:37:54 +0200

We have found a privacy/security bug in the Java implementation of the Netscape Navigator. It is very easily possible for an applet to find out the pathname of the directory in which the Netscape Navigator was started. This information could then be sent back to a CGI program for logging. Clearly this information should not be available to an applet, as is indicated by the fact that applets are prevented from reading the "user.home" and "user.dir" system properties.

When the Netscape Navigator is run under the Windows 95 OS, the pathname usually does not contain any critical information. However, when the Navigator is run under a multi-user network OS, such as UNIX, the pathname often contains the e-mail and/or login name of the user. In addition, the pathname might reveal details about the topology of the user's network, which an experienced hacker might be able to exploit.

There are two ways to protect yourself from this problem: Either start up the Netscape Navigator in a directory whose pathname does not reveal any critical information, or disable Java altogether (Options | Security Preferences | General). A system administrator can protect his network by configuring the HTTP proxy server not to retrieve Java ".class" files.

This bug is present in at least the following versions of the Navigator:

- 2.0
- 2.01
- 3.0b2
- 2.0GoldB1
- 2.01Gold

and in the implementations for at least the following platforms:

- SunOS 4.1.2, 4.1.3, 4.1.4
- SunOS 5.3, 5.4, 5.5
- Windows 95, Windows NT
- IRIX 5.2, 5.3
- HP-UX A.0903, A.0905
- Linux 1.2.10, 1.2.13
- FreeBSD 2.1.0-RELEASE
- OSF1 V3.2

We have not tested whether this bug also exists in Sun's HotJava browser.

We will release full details of the bug as soon as Sun and Netscape have issued patches which fix the problem.

Full details have been sent to Sun and Netscape. This announcements has also been posted to the "comp.lang.java" newsgroup and has been sent to CERT.

Daniel Abplanalp and Stephan Goldstein (goldstei@iamexwi.unibe.ch)
Berne, Switzerland

🔥 Swedish court fines parents for son's overly long name

Li Gong <gong@csl.sri.com>
Mon, 22 Apr 1996 23:10:42 -0700 (PDT)

It is well known that numerous computer programs are so poorly designed and implemented that they cannot handle special cases of people's names (e.g., the case of the person simply named "Smith", as in [RISKS-18.05](#)). In some other cases, there are real physical (and other) constraints that are hard to code around, such as in the case of some colleagues whose long names risk falling off the edge of their company badges.

Sometimes people just push things to far to the extreme. The Guardian Weekly reported (in the issue ending 21 Apr 1996, p.4) that "a Swedish court has fined a couple \$660 for breaking the law by naming their son Brfxxxcccxxmnpccclllmnprrxxvclmncckssqlbb11116--or Albin for short."

Does anyone know what law was broken, and can anyone decode the meaning or origin, if any, of this choice of name?

Li Gong, SRI Computer Science Laboratory, <http://www.csl.sri.com/~gong>

[Their son will be lucky if he does not get called Albin0, even the full given name might appear to be white noise.]

This is clearly job for a new Sesame Street song to help us remember the given name. PGN]

✶ Baltimore throws the book at criminals

Peter Wayner <pcw@access.digex.net>

Fri, 19 Apr 1996 17:22:03 -0400

Baltimore just finished creating a brand new technologically advanced "central booking" building where police take people after they've been arrested. Unfortunately, this heavily computerized system has become media fodder lately as people get lost in the building and are not released for days. I've seen one television news report that interviewed a woman who said she spent five days in the building because of a minor warrant for an unpaid fine. Bail was posted several times and lost.

The Thursday 18 Apr 1996 edition of the **Baltimore Sun** reports that the system is now working faster after the police started overriding the computers. For instance, there was an automated system by which prisoners could be called up for their hearings. The handheld computers that carried these messages, however, didn't work and now the City has detailed five extra officers to escort the prisoners instead.

Another woman complained that her 18-year-old retarded child was held a full day after bail was set. She says that she was speaking with booking center over the telephone when the child knocked at the door. The booking center

was telling her that her son could *not* be released until all of the computer records were complete. I can only hope that the same glitch won't let out a dangerous criminal.

The article ends by noting that the District Court Commissioner says that "Anybody [who's] been in this building would be a damn fool to [go] back to it."

✶ AMD5K86 Floating-Point Division Algorithm

J Strother Moore <moore@cli.com>

Fri, 19 Apr 96 14:28:31 CDT

I would like to bring your attention to some recent joint work by Advanced Micro Devices, Inc., and Computational Logic, Inc., in which the ACL2 theorem prover was used to prove the correctness of an algorithm of commercial interest. In particular we proved the correctness of the kernel of the floating-point division algorithm on the AMD5K86, the first Pentium-class processor produced by AMD. Roughly speaking, we proved that the algorithm implements division on the double extended precision normal and denormal numbers of the IEEE standard, in the sense that (under appropriate hypotheses) it returns the floating-point number obtained by rounding the ``infinitely precise'' quotient by the method and to the precision specified by a given rounding mode. The permitted rounding modes

include round to 0, round away from 0, round to nearest, round to positive (or negative) infinity, and ``sticky'' rounding. The proof is quite interesting, involving as it does the formalization of a lot of floating-point ``folklore'' and classical numerical analysis.

J Strother Moore

The paper may be obtained via the URL:

<http://devil.ece.utexas.edu:80/~lynch/divide/divide.html>

The title and abstract are shown below.

A Mechanically Checked Proof of the Correctness of the
Kernel
of the AMD5K86 (tm) Floating-point Division
Algorithm

J Strother Moore (Moore@cli.com)
Tom Lynch (Tom.Lynch@amd.com)
Matt Kaufmann (Matt_Kaufmann@email.mot.com)

ABSTRACT:

We describe a mechanically checked proof of the correctness of the kernel of the floating-point division algorithm used on the AMD5K86 microprocessor. The kernel is a non-restoring division algorithm that computes the floating-point quotient of two double extended precision floating-point numbers, p and d ($d \neq 0$), with respect to a rounding mode, mode. The algorithm is defined in terms of floating-point addition and multiplication. First, two Newton-Raphson iterations are used to compute a floating-point approximation of the reciprocal of d . The result is used to compute four floating-point quotient digits in the 24,,17 format (24 bits of precision

and 17 bit exponents) which are then summed using appropriate rounding modes. We prove that if p and d are 64-bit (possibly denormal) floating-point numbers, $d \neq 0$ and mode specifies one of six rounding procedures and a desired precision $0 < n \leq 64$, then the output of the algorithm is p/d rounded according to mode. We prove that every intermediate result is a floating-point number in the format required by the resources allocated to it. Our claims have been mechanically checked using the ACL2 theorem prover.

✶ MCI recommending bad security practices

Chad Ray McDaniel <chadm@unhinged.engr.sgi.com>
19 Apr 1996 21:07:06 GMT

Taking advantage of yet another incentive offer, I recently switched my long distance carrier to MCI. They sent me the standard yet-another-piece-of-plastic-to-stick-in-my-wallet calling cards. The way these cards work is that you call an 1-800 number and type in your code consisting of your phone number followed by your PIN (Personal Identification Number) which happens to be printed on the card.

Enclosed with the cards was a piece of paper in which MCI wisely suggests that you change your PIN to something other than what they assigned to you and printed on the card:

Customizing your PIN

Choosing your own four-digit number is the best way to assure you'll never forget your PIN. Make it the month and year of a loved

one's

birthday or use the same password you have for your voice mail or

computer. We'll quickly replace the PIN we assigned you with any four

digits you choose - just call 1-800-476-7306

For some strange reason MCI is recommending you to do exactly the opposite

of what good security practices would proscribe! Not only do they suggest

that you use an easily-breakable password such as an important date, but

they recommend a practice that would weaken the security of potentially more

sensitive information in a voice-mail or computer system.

Of course, what probably prompted note from MCI was a desire to prevent

MCI's customer service department from being inundated with calls from

people who forgot their PINs. This alludes to the associated risk of

requiring people to remember Yet Another Password (YAP).

-chad

⚡ Sometimes, stratum 1 time isn't so good

Dave Hsu <hsu@va.pubnix.com>

21 Apr 1996 01:16:09 -0400

I find it necessary every few weeks to set the clock on my Unix box at home

because PCs are not generally known for incorporating accurate timekeeping

hardware. Shortly before doing this recently, I ran across this notice on

the web page of the US Naval Observatory Directorate of Time,

operates a number of stratum-1 NTP servers, and is otherwise the official source of time in the United States.

<http://tycho.usno.navy.mil/phonecheck.html>

On the morning of April 16, the Directorate of Time moved its Master Clock #1 Hydrogen Maser to a new environmental chamber in Washington, D.C. Timing operations were switched to Master Clock #2

Hydrogen Maser. All except our network time servers tick and tock,

which failed to switch over, and jumped back 744.126 seconds between 12:32:58 UT and 14:23:46 UT, when the problem was corrected.

This jump was 10 million times the normal precision of these systems.

Presumably, other stratum 1 NTP servers operating from local clocks, WWV or GPS broadcasts successfully made both changeovers and never noticed. Many protocols, kerberos for instance, would not take kindly to a ten-minute drift. While the close coupling of hosts "tick" and "tock" to the actual US time standard make them appealing servers as far as nerdly bragging rights are concerned, in this instance it also made them vulnerable to the `_process_` by which US time is determined.

Dave Hsu <hsu@va.pubnix.com> Systems Programmer Software Development Group
UUNET Technologies <http://www.va.pubnix.com>

Filename bug in Windows 95

Vsevolod Ilyushchenko <SimonF@rrg.msk.su>

Tue, 23 Apr 96 20:26:16 +0400

I have found a serious bug (feature?) in Windows 95. It does not properly treat files that contain certain characters in their names. These characters include those with ASCII values of 255, 254, 249, 244, 23* and some others, all above 127. I have not found a common rule (so I probably failed the Microsoft IQ test :).

This problem was noted by Olcay Cirit in [RISKS-17.64](#) in regards to ASCII 229. He wrote that if this character is the first in a filename, then the file cannot be deleted, copied, renamed or executed. Actually, *any* of these characters at *any* place in the filename will spoil the file. Such files are visible in Explorer, with bad characters shown as underscores. You can create shortcuts to them, view their properties or even try to rename them. But any serious operation has to be performed from the command line.

A peculiarity of my DOS file managing program is that it uses direct disk access to delete files. I could not do that under Windows 95 until recently, so to deal with the "bad characters" I had to reboot into DOS prompt. Then I discovered the the "LOCK" command will allow DOS utilities to access disk directly. However, this is probably an undocumented command, it's absent in the DOS help file, and it is not an executable file.

A note for those unfamiliar with the "funny" characters. You

can enter any character at the DOS prompt by holding the Alt key and pressing the keys with digits for the character at the numeric keypad. For example, Alt+097 is 'a', and Alt+255 is one of the "bad characters". So, to see the described behaviour for yourself, create at the DOS prompt a new file that has a "bad character" in its name, then try to do something with it in Windows 95.

The RISKS? Aside from user confusion and possible pranks (which cannot do much harm, because you can always go to the command line and fix the things), there is another issue. Usually filenames with "bad characters" are not used. However, here in Russia one way of russifying a PC is to replace all those Greek, German and Swedish symbols that reside in the upper part of the ASCII table with Russian letters. So, if a Russian user had many files with Russian names, and then switched to Windows 95... Surprise, surprise! You can't manage your old files there.

I have to confess that I do not know how Russian edition of Windows 95 works. I am using the US edition.

Simon (Vsevolod Ilyushchenko) simonf@rrg.msk.su simonf@fubar.cs.montana.edu

Web page e-mail addresses Risky

Ray Normandeau <ray.normandeau@factory.com>
Sun, 21 Apr 96 22:50:00 -0500

Bell Atlantic NYNEX Mobile has a web page at: <http://www.banm.com>

>From that web page I got an e-mail address (ny@bam.com) and sent a report of a service difficulty.

I also identified my account and the dealer from which I signed up for service.

Fortunately I did NOT post my PIN number in the message.

The dealer then called me to say that my message had gone "all over the internet"!

I then e-mailed BANM again asking:

"Do private e-mail messages such as this wind up being spread all over the internet by your site?"

I was not aware of this. Why don't you warn people sending you e-mail messages that this happens.

I would assume that some of your customers would feel that this is an invasion of privacy and possibly litigatable.

BELL ATLANTIC NYNEX MOBILE has not replied yet.

I think that this should be a warning to people sending BANM what they THINK to be private e-mail messages to be advised that they may wind being published on their web page. So be sure not to put confidential information in messages to BANM.

Ray Normandeau, ray.normandeau@factory.com

<http://www.buzznyc.com/actors/res.normandeau.raymond.html>

✂ Re: Web Called "Ultimate Act of Intellectual Colonialism" (R-18.05)

Vadim Antonov <avg@sprint.net>

Fri, 19 Apr 1996 22:01:10 -0400

>Anatoly Voronov, the director of Glasnet, an Internet service provider in
>Russia, says: "It is just incredible when I hear people talking about how
>open the Web is. It is the ultimate act of intellectual colonialism. The
>product comes from America so we either must adapt to English or stop using
>it. ...

Sigh. As always clueless get most publicity.

Apparently Mr. Director of small but noisy local service provider is not aware that Russia-language newsgroup traffic is second to English-language. Apparently he's not aware that domestic ISPs in Russia offer quite a lot of Russian-language material. Apparently he does not even realize that understanding of Internet technology in Russia is good enough that there happened to be quite a few recent Russian immigrants taking senior positions in U.S. telecom industry.

The prevalence of English is merely due to the need for some common language. A modern man cannot be considered educated if he cannot read it. It's like Latin centuries ago.

How can anybody's head to be so screwed as to consider the only

real advance
in destroying the inter-cultural communication barriers to be
"the ultimate
act of intellectual colonialism" (ain't that an oxymoron?) is
beyond my
comprehension.

Maybe French government should send him a job offer.

--vadim

✶ Re: Web Called "Ultimate Act of Intellectual Colonialism" (R-18.05)

A. E. Siegman <siegman@ee.stanford.edu>

Fri, 19 Apr 1996 15:32:32 -0700

1) Nicholas (sp?) Negroponte of MIT's Media Lab begins his book
"Being Digital" by emphasizing the difference between
transporting
bits and transporting atoms. The Internet moves bits. The
Soviet
Union, in its heyday of real rather than intellectual
colonialism,
moved atoms, i.e., people, in very large numbers,
specifically natives
out of subordinated lands, Russians into them.

2) The "product", I thought, came largely from *CERN*: an
international
organization, located as it happens in *France*.

[...]

✶ Re: Euthanasia via computer (Grooby, R-18.05)

Paul Big-Ears Menon <pnm@cs.rmit.edu.au>

Sat, 20 Apr 1996 16:23:44 +1000 (EST)

I think one of the most frightening aspects of this was the penultimate screen image. There is an option "YES" (i.e., proceed) but none for "NO" (i.e., I've changed my mind).

OK, the very last screen does give you this choice, but ... how is the intended patient to know that there's another screen coming up (unless they go through a dress rehearsal)??? That screen yelled out at me from the (I think it was last Tuesday's Australian newspaper but could have been the Sun's) Computer Section page.

There was no obvious way to change one's mind.

This is the ultimate bad GUI design - no apparent option to cancel or go for a "none of the above" decision. Stupidity? Criminal? I don't know, but it was downright frightening.

It reminds me of (and I don't mean to belittle the thread) dialog boxes (or alerts) which used to notify you of a (serious) System Error on the Mac. It gave you the "choice" of doing a restart (reboot) or a quit. The trouble was that the quit almost always never worked and the thing froze anyway. Current Mac SW gives you the "choice" of restarting only (apart from those that automatically quit to the Finder).

Perhaps the subtle differences between an Alert

Where you usually don't have a choice - e.g., "You are about to

die.. Press OK to continue"

and all other forms of dialog boxes

Where you do have a choice (and even an escape hatch not covered

by those being solicited)..

need to be made more obvious. The ornamentation (at least on the Mac) for both types of displays (windows) are very similar. The windows in question (from memory) actually seemed more like web browser pages with the YES/NO options as links.

As for an escape hatch, there should always be one, regardless. It should never be out of view (ie, it should **never** be scrolled off the top).

Say, for example, a patient had a change of heart with that penultimate window displayed. OK, there's always the "quit" menu option, hitting the power switch, etc, but how comfortable and certain is he/she that this hasn't left the drip (or whatever) still in a primed state? There is no confirmation that equipment has been de-activated, especially if he/she hits the power/restart switch.

Critical systems indeed.

Paul Menon, Dept of Computer Science, Royal Melbourne Institute of Technology,
124 Latrobe Street, Melbourne 3001, Victoria, Australia +61 3 9660 3209/2348

[Various other folks commented on other aspects of this situation, testability using placebos, social implications, the long-

standing RISKS

issue of trying to solve social problems with technological solutions,

etc. All very interesting, but drifting a little too much.
TNX. PGN]

⚡ Yes, there are new Word Macro viruses, no, this isn't one of them

Rob Slade <roberts@mukluk.hq.decus.ca>

Fri, 19 Apr 1996 15:43:47 EST

In: Risks-Forum Digest Friday 19 April 1996 Volume 18 : Issue 05

>From: Edupage Editors <educom@elanor.oit.unc.edu>

>Subject: More Microsoft Viruses (Edupage, 16 Apr 1996)

>First there was the Word virus -- now there's a Word Prank Macro Virus,

Before Microsoft admitted it **was** a virus, their term for WordMacro.Concept

(the "original"), was the Word Prank Macro. This isn't new at all.

>located in a document on ActiveVRML, Microsoft's software tool for

>developing 3-D Web sites. But what's worse, is that Microsoft had to inform

>the programmers who attended its Professional Developers Conference last

>month that one of the CD-ROMs it distributed was infected. A cure is posted

Concept is everywhere. Of those who work in large corporations, the only

ones who **don't** regale me with stories of massive infestations are those

who do not know how to check for it. Microsoft has been a

repeat offender:

we are constantly hearing of new disks and CD-ROMs from MS that contain infected documents.

>on Microsoft's Web site < <http://www.microsoft.com/> >

(*Investor's Business

>Daily*, 15 Apr 1996, A8)

Microsoft's anti-WordMacro/Prank/Concept package is a Word macro itself. It

takes a piecemeal approach, and has been updated several times as new macro

viruses have been discovered. The protection provided has

holes: it is best

not to rely on it.

Edupage has had a large number of erroneous virus reports over the past year.

No worse than the general press, of course (where their material is obtained),

but somewhat disturbing in the technical community they distribute to.

roberts@decus.ca
victoria.bc.ca

rslade@vcn.bc.ca

slade@freenet.

888 Risks

"-Broomell, Russ" <MARKETING/MARKETING/RUSS%Konica_Imaging@mcimail.com>

Fri, 19 Apr 96 16:03 EST

I have spoken to several people who have signed up for the new

toll-free US 888 numbers (addition to the older 800 numbers).

They are

seeing a precursor to the year 2000 problem - many systems don't recognize

888 numbers.

One story was told that a sales person called his 888 numbered voice mail system from his hotel room. When he went to check out, he had a bill for over \$60 in phone charges. It seems that the local hotel did not recognize the prefix 888, and so assumed it was a long distance call and charged the highest toll rates. Other stories tell of pay phones that will not accept calls using 888, car phones that reject calls dialed with 888, as well as a myriad of other system related glitches.

The change seems simple - just tell your system that 888 is a valid toll free prefix. However, as with the Y2K problem, it seems that plenty of systems either were not ready for the change, or are incapable of accepting it. If this is any indication of the Y2K RISK, I'm moving to a remote mountain top in 1999.

✶ Databases without SSNs and UIDs?

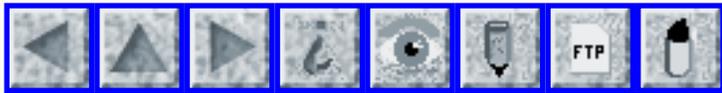
Robert Ellis Smith <0005101719@mcimail.com>

Wed, 17 Apr 96 20:26 EST

Does someone have ideas and suggestions for alternatives to the Social Security number for large organizations with large databases - methodologies like Alpha Search or Soundex? Are there other ways to manage huge databases without any use of SSNs or other numerical identifiers?

Robert Ellis Smith, Privacy Journal, Providence RI 401/274-7861

[Respond to Bob, please, and let's see if he can summarize for RISKS. 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 18: Issue 7

Thursday 25 April 1996

Contents

- [Former Oracle worker charged with perjury: bogus e-mail](#)
[PGN](#)
- [A reminder about letter bombs in MSW6.0 \[name withheld by request\]](#)
- [AOL censors British town's name!](#)
[Clive Feather](#)
[Rob Kling](#)
- [Re: Swedish court fines parents for son's overly long name](#)
[Viiveke F?k](#)
[Gunnar Pettersson](#)
- [Computers and Social Unrest](#)
[Carl Wittnebert](#)
- [When the Clock Strikes 2000](#)
[Edupage](#)
- [Re: MCI recommending bad security practices](#)
[Peter Scott](#)
- [Society and the Future of Computing '96, 16-19 Jun 1996, Snowbird, UT](#)
[Jeffrey Johnson](#)
- [CERT \(sm\) Advisory CA-96.09, Vulnerability in rpc.statd](#)
[CERT](#)
- [Info on RISKS \(comp.risks\)](#)

✦ Former Oracle worker charged with perjury: bogus e-mail

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

Tue, 23 Apr 96 17:58:50 PDT

Adelyn Lee had won a \$100K out-of-court settlement for wrongful termination from Oracle in February 1995, claiming that she had been fired for refusing to have sex with Oracle president Larry Ellison. She had apparently used as evidence a piece of e-mail from her boss VP Craig Ramsey to Ellison, confirming that Lee had been terminated as per Ellison's request. To make a long story short, San Mateo County Deputy District Attorney Paul Wasserman said that their investigation has now come to the conclusion that Ramsey could not have sent the e-mail (because he was driving in his car at the time according to cell-phone records) and that, as Ramsey's executive assistant, Lee knew his passwords (and indeed had been responsible for changing them for him periodically). Lee has now been charged with felony perjury for lying and sending false e-mail. [Source: *San Francisco Chronicle*, 20 Apr 1996, D1-2]

What are some of the conclusions for RISKS readers (not new)?

1. Don't believe e-mail FROM: headers accurately represent the sender.
2. Don't believe the content of e-mail, whether or not the headers are correct.
3. Don't share your passwords overtly with anyone, or let someone else

be responsible for your passwords.

4. Don't use covertly compromisable reusable fixed passwords; how often

you change them is more or less irrelevant.

5. Use one-time nonreusable authentication tokens instead of fixed passwords.

6. Even if you use PEM, PGP, stronger-crypto e-mail, or whatever, you

cannot ensure authenticity, because of untrustworthy operating systems

and untrustworthy users.

7. Beware of trying to use e-mail as nonrepudiatable court evidence.

8. HOWEVER, don't believe that cell-phone records are valid as court

evidence; they too could be bogus or altered. If someone drags you

into court, find someone who can demonstrate how easily those records

could have been altered!

9. Etc., etc., etc.

✶ A reminder about letter bombs in MSW6.0

<"[name withheld by request]">

Tue, 23 Apr 96 17:58:50 PDT

Today I got e-mail from Agptacek@aol.com. I have never received e-mail from

this account before. I have no idea who it is. All I got was the message

below --- "Pls. find file attached." --- plus a Microsoft Word 6.0 file.

Now, anybody who has been following the stuff with MSW6.0 knows that

executable code can be hidden in MSW6.0 files. Perhaps code to delete my

files. Or give me a new virus. [Or a nasty Trojan horse.]

Do you trust e-mail that anybody sends you?

```
>From: Agptacek@aol.com
>Date: Wed, 24 Apr 1996 01:02:03 -0400
>To: *****
>Subject: Discovery Records
>MIME-Version: 1.0
>
>Content-ID: <0_18723_830322121@emout07.mail.aol.com.30083>
>Content-type: text/plain
>
>Pls. find file attached.
>
>Content-ID: <0_18723_830322121@emout07.mail.aol.com.30084>
>Content-type: application/applefile;
>    name="Discovery";
>    X-Mac-Creator="4d535744";
>    X-Mac-Type="5736424e"
>
>Attachment converted: Asher:Discovery 1 (W6BN/MSWD) (00008B8A)
```

⚡ AOL censors British town's name!

Clive Feather <cdwf@cityscape.co.uk>

Wed, 17 Apr 1996 15:28:52 +0100 (BST)

[Clive forwarded to RISKS an long item from the Computer underground Digest,

Thu Apr 11, 1996, Volume 8 : Issue 29, ISSN 1004-042X, from Doug Blackie

<STEELBEAT@aol.com> that relates an experience Doug had in trying to

register with AOL. He entered his name "Blackie" and his home town

"Scunthorpe", and found that AOL's (indecenty-filtering) registration

program would not accept that combination. After various discussions with

the AOL folks in Dublin, he discovered that he could register

properly if

he entered the town as "Sconthorpe". As a result of this curious situation,

AOL has announced that the name of the town will henceforth be known as

"Sconthorpe". The entire saga is documented in the Scunthorpe Evening

Telegraph (final edition) of Tuesday, 9 Apr 1996, issue number 30111,

printed and published by Grimsby and Scunthorpe Newspapers Ltd., Telegraph

House, Doncaster Road, Scunthorpe, DN15 7RE, UK. The article was provided

on-line by David G. Bell <dbell@zhochaka.demon.co.uk>, and was included as

a part of Doug Blackie's message. PGN Abstracting.]

⚡ Re: AOL censors town's name!

Rob Kling <kling@ics.uci.edu>

Thu, 25 Apr 1996 11:10:22 -0700

[The previous item contributed by Clive Feather touches on some further

serious issues relating to the effectiveness, propriety, and risks

involved in filters that attempt to censor on the basis of linguistic

strings; as other examples, side-effects of filtering "couples" ([RISKS-17.79](#)) and "xxx" (SurfWatch, [RISKS-17.81](#)) have been noted in recent

RISKS postings.

Rob Kling is a member of the ACM Committee on Computers and Public Policy,

the umbrella organization in ACM for RISKS. He had the following comments

upon seeing the above message; his comments address just a few of the RISKS

issues raised. PGN]

There is a lot of info regarding Scunthorpe obtainable via Alta Vista.

This is a real city and its integrity deserves respect, even if it is

not exactly a place well-known to people in the US. [For example, see

<http://www.computerprint.co.uk/scunthorpe/travel.html> and <http://www.computerprint.co.uk/scunthorpe/history.html> .]

I can imagine that there might even be some people with the last name of

Scunthorpe. The willingness of AOL (or other services) to excise identities

in the name of "decency" raises big issues of genuine decency in my view.

Rob Kling

✶ Re: Swedish court fines parents for son's overly long name

?= a letter UNIX can't handle) <viiveke@isy.liu.se (Viiveke F?k>

Wed, 24 Apr 1996 08:52:41 +0200

The law in question states that parents should report the name they have

chosen for their children within a specified time after birth (three months

I think). The authorities in their turn has a rule saying that they should

not allow registration of names that are likely to cause harassment or other

obvious drawbacks for the child, like giving a girl what is traditionally

exclusively a boy's name and vice versa. Another recent case was when

parents were not allowed to name their girl Ikea (a constructed name for a

fairly well-known furniture company) and an older example was when another girl could not be named Veranda (which means exactly the same in Swedish).

What has this got to do with computers and risks? The parent's choice of name in this case is a protest against bureaucracy in general, one part of which is that the authorities have indeed a limit on how many characters that they register for each child. (The row of letters is as impossible to pronounce in Swedish as it is in English. Albin is of course a perfectly valid name here too.)

As for computers and real risks, this is an international question about assumptions of name structure and their use in design of computer systems. We often even can't handle our own in Sweden. Swedes for example typically have from one to three first names, and they choose themselves which one that they use daily. That choice is reported, but many computer systems do not register it. Normally it is the first "first name", but not necessarily. Which means that there are mix-ups, when for example a computer sends a letter to George Thomas Smith addressed to "George Smith", and that happens to be what the father is not called (he uses his second name Thomas) but it also happens to be what the son (Andrew Charles George Smith) actually is called. This happened in my husband's family, and guess how much trouble there was when the son tried to report that he was moving to a new address... As for myself, I sometimes give in and register my second "first name" as "middle name" when travelling, so that

passport

authorities do not complain that I do have a "middle name" and should fill it in. But if you come to Sweden and marry someone here, it is very likely that you can not register that child's middle name, because it is "offensive" as a first name, and we only register first and family names.

Viiveke F=E5k, Department of Electrical Engineering, Link=F6ping University
S-581 83 Link=F6ping Sweden +46 13 281722 Viiveke@isy.liu.se

[Incidentally, Albin's would-be given name (noted in [RISKS-18.06](#))

had one occurrence of the putatively heinous "xxx". Perhaps we will all someday have to be identified by multilingually and transnationally filtered globally biunique identifiers -- to accommodate our computer systems. (Note that Internet addresses and phone numbers are unique if globally qualified, but are not biunique -- because they may be shared by multiple personalities). PGN]

✶ Re: Swedish court fines parents for son's overly long name (R-18.06)

Gunnar Pettersson <gunnar.pettersson@powrd.demon.co.uk>
Thu, 25 Apr 1996 16:59:09 +0000

The law that was broken is the Swedish 'Name Law' (SFS 1982:670) and the authority which deals with its implementation is the Swedish Patent & Registration Office.

Not having seen the detailed judgement in this case, I would guess that the law was seen to have been broken in at least two ways. First a

technical

reason: as your correspondent surmises, the name would have been regarded

as far too unmanageable for inclusion in the computerized Civic Registration data held on all Swedish citizens. Secondly, and perhaps more

importantly, the law explicitly prohibits forenames "which can cause

offence, or may lead to any inconvenience for the bearer, or is for any

other reason obviously unsuitable as a forename".

As far as the meaning of the name 'Brfxxx...' is concerned, I would have

thought it is to be found precisely in its lack of meaning. And, whatever

one thinks of a law like the Swedish one, what about the poor kid himself?

Cases like this one tend to prove very little about the law itself, and much

more about the pretty warped attitude some people have towards their

offspring...

The Swedish name law, on which most other Nordic name laws are based, is

nonetheless unusually restrictive as far as choosing and changing names are

concerned. However, it should be pointed out that practically every other

country, with the exception of the UK and parts of the US, have *some* form

of restriction on names: e.g. Germans can't change their names to Hitler;

French forenames must be taken from saints and/or antiquity; etc. etc.

In Nov 1992, I wrote and presented a talk on BBC radio, "Names Never Hurt

You", which deals with the social and political aspects of name laws, with

particular emphasis on Sweden. If anyone would like a transcript, please

e-mail me.

✶ Computers and Social Unrest

Carl Wittnebert <cewit@wco.com>

Thu, 25 Apr 1996 04:09:05 -0700 (PDT)

A potentially earthshaking risk of using computers is currently being discussed at the highest levels of the U. S. government. The risk involves human skill obsolescence, a growing wage gap between skilled and unskilled workers, and possible social unrest. The phenomenon may underlie the themes of economic nationalism and protectionism that have surfaced during the current Presidential campaign.

The **Wall Street Journal** devoted a front-page column to the topic on 22 Apr 1996. It quoted Federal Reserve Board Chairman Alan Greenspan as saying, "Human skills are subject to obsolescence at a rate perhaps unprecedented in American history." It went on to quote George David, chief executive officer at United Technologies Corp., who believes that 18 million U.S. workers are "at risk" because their jobs are "prone to automation."

Upheaval in the nature of work--in manufacturing in the 1980's, and now in the service sector--has been discussed for some time, usually under the assumption that additional jobs would be created to replace the ones lost to machines. Increasingly, the question is arising as to just how much the new jobs are going to pay.

⚡ **When the Clock Strikes 2000 (Edupage, 23 Apr 1996)**

Edupage Editors <educom@elanor.oit.unc.edu>

Tue, 23 Apr 1996 17:34:05 -0400 (EDT)

The Gartner Group in Stamford, Connecticut, says the federal government will spend about \$30 billion to modify a massive number of computer programs in which years were coded simply as two-digit numbers (without identifying the century) and which will have to be fixed so that they can correctly calculate things like benefits payments. It is also estimated that by the time the year 2000 comes around only 70% of government computer programs will have been modified to deal with the problem. (*Computerworld*, 22 Apr 1996 p1)
[See [RISKS-17.82](#) for global estimates of something around half a trillion dollars, also from the Gartner Group. PGN]

⚡ **Re: MCI recommending bad security practices (McDaniel, [RISKS-18.06](#))**

Peter Scott <pjscott@euclid.Jpl.Nasa.Gov>

Wed, 24 Apr 1996 09:33:51 -0700

> For some strange reason MCI is recommending you to do exactly the opposite
> of what good security practices would proscribe! Not only do they suggest

^

Now there's an example of a misspelling-type RISK [reversing the meaning!].

Peter Scott, NASA/JPL/Caltech Peter.J.Scott@jpl.nasa.gov

⚡ Society and the Future of Computing '96, 16-19 Jun 1996, Snowbird, UT

Jeff Johnson <Jeffrey.Johnson@Eng.Sun.COM>

Thu, 25 Apr 1996 10:06:56 -0700

Society and the Future of Computing '96
June 16-20, 1996
Cliff Lodge
Snowbird, Utah

<http://www.lanl.gov/SFC>

Sponsor: USACM. Contact Rick Light, Los Alamos National Lab, MS B294,

Group CIC-7, Los Alamos, NM 87545, phone 505/667-0744, e-mail rxl@lanl.gov, Web: <http://www.lanl.gov/SFC/96/sfcHome.html>.

This conference provides a multidisciplinary forum to articulate novel research directions that advance computer science in ways that are truly beneficial to society. Participants will share, explore, and demonstrate the responsible use of advanced scientific computing and National Information Infrastructure (NII) Program technologies for the benefit of diverse communities.

The conference structure includes keynote speakers, panels of invited speakers in which attendees and the panelists engage each other in open discussions of the issues, interactive poster presentations, debates, and

workshops. The intent is to share ideas in a multidisciplinary environment for mutual enrichment and learning, ultimately to affect the directions of computer science research and applications for the benefit of all. The conference Web site includes the preliminary conference agenda and will continue to provide the latest information as the conference design unfolds.

Keynote speakers:

Tom Landauer, U. of Colorado (Boulder): "Computers, Usefulness,

Usability, Productivity, and Happiness"

Laura Breeden, formerly of of US Commerce Dept. NTIA: "Whose

Voice is Heard? Listening to the Computer and Communications Revolution"

Bill Wulf, University of Virginia: "Information Technology is the Lever, But Where Shall We Stand?"

Panels:

Creating the Future: Computer Industry Research Lab Heads
Rick Light, Moderator

Working in the Networked Economy: Issues
Gary Chapman, Moderator

Working in the Networked Economy: Opportunities
Phil Agre, Moderator

Contrasting Images of the Future
Allan Kuchinsky, Moderator

The European Information Society (live from Europe)
Terry Bynum, Moderator

If Anyone Can Publish, Who Will Edit?
Karen Coyle, Moderator

On the Internet, No One Knows You're a Dog
Brenda Allen, Moderator

Government On-Line: Report Card and Futures
Charles Brownstein, Moderator

Workshops:

Shneiderman: "The Durango Declaration Continued: Toward a Snowbird Conference Statement"

Cisler, Uncapher, Press: "Implications of the Net for Industrialized

Countries, Developing Nations, and Indigenous Cultures"

Epstein: "Emerging Realities, Virtual and Otherwise"

Meyer: "Anthropology and Computer Technologies"

✦ CERT (sm) Advisory CA-96.09, 24 Apr 1996, Vulnerability in rpc.statd

CERT Advisory <cert-advisory@cert.org>

Wed, 24 Apr 1996 14:25:09 -0400

The CERT Coordination Center has received reports of a vulnerability in rpc.statd (rpc.statd is also known as statd on some systems). As of the date of this advisory, we have received no reports of this vulnerability being exploited.

If exploited, this vulnerability can be used to remove any file that the root user can remove or to create any file that the root user can create.

Section III and Appendix A contain information from vendors. Appendix B contains an example of a possible workaround.

As we receive additional information relating to this advisory, we will place it in

ftp://info.cert.org/pub/cert_advisories/CA-96.09.README

We encourage you to check our README files regularly for updates on advisories that relate to your site.

I. Description

rpc.statd, also called statd, is the NFS file-locking status monitor. It interacts with rpc.lockd, also called lockd, to provide the crash and recovery functions for file locking across NFS.

NFS is stateless, which means that NFS clients and servers can be rebooted without a loss of file integrity due to NFS. In contrast, NFS file locking is stateful. To achieve this stateful nature in a stateless environment, rpc.lockd must work with rpc.statd to add state to file locking.

To understand what rpc.statd does, it is first necessary to understand what rpc.lockd does. rpc.lockd processes lock requests that are sent either locally by the kernel or remotely by another lock daemon. rpc.lockd forwards lock requests for remote NFS files to the NFS server's lock daemon using Remote Procedure Calls (RPC).

rpc.lockd then requests monitoring service from the status monitor daemon, rpc.statd, running on the NFS server. Monitoring services are needed because file locks are maintained in the NFS server kernel. In the event of a system crash or reboot, all NFS locks would normally be lost. It is rpc.statd that adds stateful file locking.

When an NFS server reboots, rpc.statd causes the previously held locks to be recovered by notifying the NFS client lock daemons to resubmit

previously granted lock requests. If a lock daemon fails to secure a

previously granted lock on the NFS server, it sends SIGLOST to the

process that originally requested the file lock.

The vulnerability in rpc.statd is its lack of validation of the

information it receives from what is presumed to be the remote rpc.lockd.

Because rpc.statd normally runs as root and because it does not validate

this information, rpc.statd can be made to remove or create any file that

the root user can remove or create on the NFS server.

II. Impact

Any file that root could remove can be removed by rpc.statd. Any file

that root could create can be created by rpc.statd, albeit with mode 200.

III. Solution

The general solution to this problem is to replace the rpc.statd daemon

with one that validates the information sent to it by the remote

rpc.lockd. We recommend that you install a patch from your vendor if

possible. If a patch is not available for your system, we recommend

contacting your vendor and requesting that a patch be developed as soon

as possible. In the meantime, consider whether the information in

Appendix B is applicable to your site.

Vendor Information

Below is a summary list of the vendors who have reported to

us as of the
date of this advisory.

Patch information and other details are in Appendix A of
this advisory
and reproduced in the CA-96.09.README file. We will update
the README
file as we receive more information.

If your vendor's name is not on this list, please contact
the vendor
directly.

Vendor	Status
-----	-----
Apple Computer, Inc. 3.1.1 and the Apple	vulnerable - A/UX version earlier; AIX 4.1.4 for Network Server
Berkeley Software Design, Inc. Cray Research, Inc. version 9.0 and	not vulnerable - BSD/OS vulnerable - Unicos
Data General Corporation Digital Equipment Corporation V3.0 through through V4.5	higher vulnerable - DG/UX R4.11 vulnerable - UNIX (OSF/1) V3.2d; ULTRIX V4.3
Harris Computer Systems Corp. of NightHawk	vulnerable - all versions
versions of CyberGuard CX/SX	CX/UX and PowerUX not vulnerable - all
Hewlett-Packard Company IBM Corporation 4.1	NightHawk CX/SX and vulnerable - 9.X and 10.X vulnerable - AIX 3.2 and
NEC Corporation NeXT Software, Inc. before 4.0;	some systems vulnerable vulnerable - versions

The Santa Cruz Operation, Inc.
UnixWare 2.x.;

SCO Open Desktop

Silicon Graphics, Inc.
of IRIX except

Sony Corporation
4.2.1, 6.0.3, 6.1,

Sun Microsystems, Inc.
- SunOS 4.x

will be fixed in 4.0
not vulnerable - SCO

SCO OpenServer 3.0, 5;

2.x, 3.x; SCO NFS 1.x.x.
vulnerable - all versions

6.2
not vulnerable - IRIX 6.2
vulnerable - NEWS-OS

and 6.1.1
believed to be vulnerable

and Solaris 2.x

The CERT Coordination Center thanks Andrew Gross of the San Diego Supercomputer Center for reporting this problem and Wolfgang Ley of DFN-CERT for his support in responding to this problem.

If you believe that your system has been compromised, contact the CERT Coordination Center or your representative in the Forum of Incident Response and Security Teams (FIRST).

We strongly urge you to encrypt any sensitive information you send by email. The CERT Coordination Center can support a shared DES key and PGP. Contact the CERT staff for more information.

Location of CERT PGP key

ftp://info.cert.org/pub/CERT_PGP.key

CERT Contact Information

Email cert@cert.org

Phone +1 412-268-7090 (24-hour hotline)

CERT personnel answer 8:30-5:00 p.m. EST (GMT-5)/EDT(GMT-4), and are on call for emergencies during other hours.

Fax +1 412-268-6989

Postal address

CERT Coordination Center
Software Engineering Institute
Carnegie Mellon University
Pittsburgh PA 15213-3890 USA

CERT publications, information about FIRST representatives, and other

security-related information are available for anonymous FTP from

<http://www.cert.org/>

<ftp://info.cert.org/pub/>

CERT advisories and bulletins are also posted on the USENET newsgroup

comp.security.announce

To be added to our mailing list for CERT advisories and bulletins, send your

email address to

cert-advisory-request@cert.org

Copyright 1996 Carnegie Mellon University

This material may be reproduced and distributed without permission provided it

is used for noncommercial purposes and the copyright statement is included.

CERT is a service mark of Carnegie Mellon University.

[Appendices removed 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 18: Issue 8

Monday 29 April 1996

Contents

- [Another way to run native code from Java applets](#)
[David Hopwood](#)
- [The T-43A Accident in Dubrovnik](#)
[Peter Ladkin](#)
- [FAA drops navigation system contract](#)
[Fred Ballard](#)
- [The RISK of attributing error to malice](#)
[Paul R. Potts](#)
- [Need to censor AOL's name!](#)
[Jack Campin](#)
- [Re: AOL censors town's name!](#)
[Flavian Wallis](#)
[Greg Gomberg](#)
[Philip Overy](#)
- [The "finger" command and "Paul Hilfinger"](#)
[Jim Horning](#)
- [Re: Swedish and French names](#)
[Bertrand Meyer](#)
- [Re: MCI recommending bad security practices](#)
[Andy Piper](#)

- [Re: Former Oracle worker ... bogus e-mail \(Mike Marler, J.R.Valverde jr\)](#)
[John C. Rivard](#)
[Simona Nass](#)
[Steve Kilbane](#)
 - [Coordination and Administration of the Internet: workshop CFP](#)
[Tim Leshan](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ Another way to run native code from Java applets

David Hopwood <david.hopwood@lady-margaret-hall.oxford.ac.uk>
Sun, 28 Apr 1996 03:42:49 +0000 (BST)

In addition to the security bug found by Drew Dean, Ed Felten and Dan Wallach in March, there is another way to run native code from a Java applet, which will require a separate fix to the current versions of Netscape (2.01 and Atlas PR2) and Sun's Java Development Kit (1.01).

Both this attack and the previous one rely on an applet being able to create an instance of the same security-sensitive class, but each does so using an independent hole in the bytecode verifier.

Once an applet is able to run native code, it can read, write, and execute any local file, with the permissions of the browser. These attacks do not require any additional preconditions, other than viewing the attacker's web page with Java enabled. They can be done without the user's knowledge.

Summary of Java bugs found so far

~~~~~

| Date      | Found by | Fixed in                | Effects                                                                                                                               |
|-----------|----------|-------------------------|---------------------------------------------------------------------------------------------------------------------------------------|
| -----     | -----    | -----                   | -----                                                                                                                                 |
| Oct 30 95 | DFW      | not fixed<br>in HotJava | Various - see<br><a href="ftp://ftp.cs.princeton.edu/reports/1995/501.ps.Z">ftp://ftp.cs.princeton.edu/<br/>reports/1995/501.ps.Z</a> |
| Feb 18 96 | DFW/SG   | 1.01/2.01               | Applets can exploit DNS spoofing<br>to<br>connect to machines behind<br>firewalls                                                     |
| Mar 2 96  | DH       | 1.01/2.01               | Buffer overflow bug in javap<br>win32/MacOS: Applets can run<br>native code                                                           |
|           |          |                         | UNIX: Ditto, provided<br>certain files can<br>be created on the<br>client                                                             |
| Mar 22 96 | DFW      | not fixed               | Applets can run native code                                                                                                           |
| Mar 22 96 | EW       | not fixed               | If host names are unregistered,<br>applets may be<br>able to connect to them                                                          |
| Apr 27 96 | DH       | not fixed               | Applets can run native code                                                                                                           |

There was also a separate bug in beta versions of Netscape 2.0 which, in hindsight, would have allowed applets to run native code.

[DFW = Drew Dean, Ed Felten, Dan Wallach  
<http://www.cs.princeton.edu/sip/News.html>  
SG = Steve Gibbons  
<http://www.aztech.net/~steve/java/>  
DH = David Hopwood  
<http://ferret.lmh.ox.ac.uk/~david/java/>  
EW = Eric Williams  
<http://www.sky.net/~williams/java/javasec.html>

Dates indicate when the problem was first posted to RISKS, except for Eric Williams' bug, which has not been posted.]

For bugs in Javascript, see John LoVerso's page  
<http://www.osf.org/~loverso/javascript/>

These include the ability to list any local directory (apparently fixed in Atlas PR2), and a new version of the real-time history tracker.

Additional information on the March 2nd absolute pathname bug is now available from

<http://ferret.lmh.ox.ac.uk/~david/java/>

Recommended actions

~~~~~

Netscape (2.0beta*, 2.0, 2.01):

Disable Java (on all platforms except Windows 3.1x), and if possible

Javascript, using the Security Preferences dialogue in the Options menu.

Note that the section on security in the Netscape release notes is not up-to-date.

Netscape (Atlas PR1, PR2):

As above, except that the options to disable Java and Javascript have moved to the Languages tab in the Network Preferences dialogue.

Appletviewer (JDK beta*, 1.0, 1.01):

Do not use appletviewer to load applets from untrusted hosts.

HotJava (alpha*):

Sun no longer supports HotJava alpha, and does not intend to fix

any of its security holes until a beta version is released.

David Hopwood david.hopwood@lmh.ox.ac.uk

The T-43A Accident in Dubrovnik

<ladkin@TechFak.Uni-Bielefeld.DE>

Mon, 29 Apr 1996 21:56:27 +0200

There are many articles in RISKS wondering about various aspects of the safety of increasing automation in aircraft. We should remember that increased automation can also help to avoid accidents.

Nancy Leveson ([RISKS-17.21](#)) pointed out some incidents in which TCAS (the Traffic Avoidance and Collision Alert System) seems to have helped avoid collision accidents. In [RISKS-17.89](#), I referred to a report that the US Navy was speeding up acquisition of digital flight control systems for F-14s to help avoid loss-of-control accidents.

There is another example in recent news. From newspaper reports, it seems as if the safety of flight IFOR 21, a US Air Force T-43A (a type of B737-200) which crashed on approach to Dubrovnik, Croatia, could have been enhanced by more modern navigation equipment. This flight carried US Secretary of Commerce Ron Brown.

The USAF does not normally release results of its investigations to the public. So I have summarised facts from a short *Washington Post* article, two articles from *Flight International*, and a *New York Times Service* feature article that appeared in the *International Herald Tribune* on Monday 29 Apr 1996. I also include some of my own observations and (a link to) the approach plate (map) for the Dubrovnik NDB Runway 12 approach that the aircraft was in course of executing. This summary is available in the Compendium `Computer-Related Incidents and Accidents...' under my WWW home

page at <http://www.techfak.uni-bielefeld.de/~ladkin/>

Peter Ladkin

[Archivists reading RISKS ten years from now will hope that it is **still** there then. But Peter's home page is clearly a moving target anyway, changing at flying speeds. Grab it while it's hot. PGN]

✶ FAA drops navigation system contract

Fred Ballard <72400.1525@CompuServe.COM>
29 Apr 96 10:13:30 EDT

Citing cost overruns and schedule delays because of mismanagement, the Federal Aviation Administration canceled a \$475 million contract that was intended to help the airlines get extremely precise navigational data from satellites. The FAA announced the contract in August with Wilcox Electric Inc. of Kansas City, a subsidiary of Thomson-CSF SA of Paris. The FAA said the action was part of a new strategy of cutting losses early, rather than struggling along for years with mounting delays and cost overruns.

The Minneapolis Star Tribune, Saturday, April 27, 1996, p. A8.

✶ The RISK of attributing error to malice

Paul R. Potts <potts@cancer.med.umich.edu>
Mon, 29 Apr 1996 12:09:03 -0400

I'm writing this up as a reminder re: the importance of not jumping to conclusions, especially when computers are involved. My hope is that perhaps this story will one day be recalled by a reader facing a similar situation, and a better outcome will result.

Recently, one of our staff members found an incomplete outgoing message in her e-mail that she did not write. The appearance was that another staff member might have been forging an e-mail message from her machine, but been interrupted. The creation date was several days before the message was found, making it appear that the creation date had been faked; there were two copies of the message in two locations, making it appear that the message had been copied; the writing style was not that of the machine's owner; the issue mentioned was one that had a bone of contention between the staff members days earlier.

In my initial investigation, I reported that without full security and a reliable audit trail it wasn't really possible to prove that such a forgery had been done, but that this did look suspicious. Relationships within our group had been strained, and this was enough to start accusations flying. The climate in the office, already toxic, grew poisonous.

Yesterday, I put my finger on the actual smoking gun: I hadn't known it initially, but the two staffers were using Macintosh file sharing and one was mounting the entire hard disk of the other as a server volume using the

owner password, which gave complete read and write access to the entire volume. This was counter to our written guidelines on safe file sharing.

The mail program in question, poorly-written, stores full path names to keep track of the folder where it creates outgoing mail. One system's internal hard disk had been renamed from the default "Macintosh HD" and the other had not - I'm sure most readers know by now where this is going.

The mail program found its outgoing messages folder on the wrong machine and the message in question was created there. I replicated this exact sequence of events on two other machines yesterday while my supervisor watched. I haven't explained the duplicate copies on the remote machine or why the message was seen earlier, but this isn't necessary in order to convince me that this "forgery" was really an accident.

Upon reflection, there was no clear motive, and everyone agrees now that if the attempt had been to defame a fellow employee, a much more coherent and effective job would have been done. Public apologies have been made. We're switching e-mail clients and our staff members will be expected to follow guidelines for safe file-sharing. I personally was far, far too willing to blame a staff member before exhausting every technical possibility. Now we've got to work at building a trusting work environment again, and hope that this can be put behind us, but I don't think the accused staff member will quickly forget being the target of an unfair accusation where the only evidence existed on a computer, and my confidence in my own

judgment has
been badly shaken.

The RISK is of attributing to malice what is easily attributable to poorly-written software, incomplete understanding of the system your co-workers use, and failure to follow good security practices. There is a further risk that a pre-existing climate of suspiciousness can push an investigation of an anomaly into a witch hunt. The last RISK is that it is too easy for someone like myself, inexperienced at managing conflicts between staff members, to lose his objectivity and start becoming more suspicious of a person than of a computer. As a regular RISKS reader, I should have known better.

"Paul R. Potts" potts@cancer.med.umich.edu>, Technical Lead,
Health Media Research Lab, University of Michigan Comprehensive
Cancer Center

⚡ Need to censor AOL's name! (Re: [RISKS-18.07](#))

Jack Campin <jack@purr.demon.co.uk>
Sat, 27 Apr 1996 14:48:50 +0000

I can't wait for AOL to try this with other languages. The "am" in "America" means the same in Turkish as what they're objecting to in Scunthorpe. Perhaps they need to transform themselves to "Omerica On-Line"!

The first time I ever saw the offending word in print, it was spelled with

an "o" anyway; this was in the early 60s in a script in `_Plays`
and `Players_`,
a British magazine devoted to contemporary drama. They
presumably did that
to get by the English drama censor (the Lord Chamberlain, whose
idiosyncratic prohibitions provided the British intelligentsia
of the time
with nearly as much amusement as their modern American
counterparts get from
the CDA).

✉ Re: AOL censors town's name! ([RISKS-18.07](#))

Flavian Wallis <flavian@evanston.lib.il.us>

Sun, 28 Apr 1996 00:03:54 -0500

It seems somewhat ironic that AOL's substitution of an 'o' for a
'u' in the
name of Scunthorpe has just translated the problem -- turning an
embedded
English vulgarity into a French one, the same one just to add to
the fun
(what my dictionary refers to delicately as: "Vulg. Sexe de la
femme.")

AOL, or any other organisation applying such a policy on a
global basis,
runs the risk of altering a name to avoid a perceived English
vulgarity and
creating as much, if not more, offense in the language and
culture of
origin. This is complicated by the fact that these second-order
vulgaritys
would likely be unrelated to the English obsession with body
parts and
functions and thus be much harder for the censor to detect.

Flavian Wallis

⚡ Re: AOL censors town's name! ([RISKS-18.07](#))

Gomberg Greg <GombergG@logica.com>

Fri, 26 Apr 96 12:39:00 bst

Fans of British humour will recall that "Norwich" encodes an indecent suggestion. Perhaps AOL should be censoring that fine city's name also.

Greg

[Lots of other comments were received as well, including the common

gerundive name of a German town, a few classical typos that made things

worse in miscorrection, and more. This thread is certainly not unraveling. PGN]

⚡ Re: AOL censors British town's name! ([RISKS-18.07](#))

Philip Overy <pjo33@mailbox.rl.ac.uk>

Fri, 26 Apr 1996 12:20:13 +0100

[Long message excerpted for RISKS ...] The real message is:

- 1) Use PGP.
- 2) If you receive PGP e-mail and find it to be offensive, and only that, give up corresponding with the person in question.
- 3) (which is the crux of the matter) Does the e-mail contain a serious threat or form of intimidation?, in which case it is covered by the

normal strictures against intimidation, does it contain
slanders or
libels (N.B. English law doesn't consider a statement of fact
to be a
slander or libel, so I don't in all honesty think this law
counters
freedom of speech, even though its heavier users are Tory
MPs)? and
finally is it in some other way criminal?, e.g., a chain
letter to
deprive you of all your cash, which I admit I tend to dismiss
as being
the "buyer"'s problem to worry about - AOL aren't protecting
you from ANY
of these rather larger problems.

and the message to America On Line is that they should probably
provide
something on the lines of PGP, however ropy and possible to
crack, and stop
fooling around with people's e-mail and free speech. IBM must
have had this
problem, because under VM it was possible to monitor only your
own id, not
the id of someone you managed - a lesson I think Unix should
probably have
learned too (as a result a VM manager could claim not to be
responsible for
the nasty activities of the users). [...]

Phil Overy

⚡ The "finger" command and "Paul Hilfinger"

Jim Horning <horning@hector.mti.sgi.com>

Mon, 29 Apr 1996 12:03:42 -0700

The AOL censorship item in [RISKS-18.07](#) reminds me of Paul
Hilfinger's story

about the time the Carnegie-Mellon University computer-center staff was ordered by the CMU administration to change the name of the "finger" command (despite it being an ARPAnet standard). They changed "finger" to "where" and also took it upon themselves to change Paul's name to "Paul Hilwhere" (initially intending it to be temporary). Paul actually approved of the change (as a kind of gentle protest), and it remained that way for some time.

Jim Horning

⚡ Re: Swedish and French names (Pettersson, [RISKS-18.07](#))

<Bertrand.Meyer@eiffel.com>

Fri, 26 Apr 96 10:48:35 PDT

> French forenames must be taken from saints and/or antiquity ...

Funny about how French mores are constantly misrepresented in the Anglo-Saxon world - usually to present France as a kind of Soviet Union

where everything is government-regulated.

The informal guideline until a few years ago was that the name should either be from antiquity or appear in some calendar. This includes religious calendars (not only Catholic), but also e.g. the Revolutionary calendar, where months appear with names like Nivose and Ventose, and days have names like Cerise (cherry). I believe all the law said was something like local authorities should exert proper care; the calendar approach was

a pragmatic way to resolve borderline cases. In last resort, of course, the courts would decide.

In the past twenty years or so pragmatism has reigned, what with the large immigrant populations (if you go to a playground you'll hear parents calling "Leila" and "Tarik" all around - not typical Catholic saint names), the influence of American movies (every other child seems to be called Jessica or Gregory), and a general move towards more laxity in tolerating individual tastes. This clearly has some limits, and I don't think that 'Brfxxx...' would pass any more there than in Sweden.

-- Bertrand Meyer, ISE Inc., Santa Barbara

This posting adheres to the SELF-DISCIPLINE guidelines for better USENET discussions. See <http://www.eiffel.com/discipline>.

Re: MCI recommending bad security practices (McDaniel, RISKS-18.06)

Andy Piper <andyp@wrath>
Fri, 26 Apr 1996 11:32:02 +0100

>> of what good security practices would proscribe! Not only do they suggest
>> ^

Even more interesting is the fact that I use a proportional spaced font for reading news/editing etc and so the '^' character appeared under the word 'practices' rather than 'proscribe'. I stared at

it for
ages before realising what had happened.

The RISKS? Don't make assumptions about how your intended audience will view information. We constantly have problems with this - people using MS-Word as an e-mail format; non mime-compliant mail readers; compression/encoding schemes that are UNIX-unfriendly - the list is endless.

andy piper

✉ Re: Former Oracle worker ... bogus e-mail ([RISKS-18.07](#))

Mike Marler <Mike.Marler@oit.gatech.edu>

Fri, 26 Apr 1996 09:50:11 -0400 (EDT)

9a. Don't believe that a person cannot have a batch job or background process running on their machine, which could send e-mail to another address (with or without "fudged headers"), while the person is, for example, 5 miles offshore of Costa Rica catching sailfish.

9b. Don't believe that a person cannot have an automated answering service that sends a reply to "a piece of e-mail" stating something similar to the following: "Sorry I cannot send a detailed reply to your 'piece of e-mail', because I will be very busy in meetings until the end of today". When the actual person is "playing hookey" or still chasing those sailfish in Costa Rica.

Mike Marler, Information Technology, Georgia Tech, Atlanta, Georgia 30332-0715 mike.marler@oit.gatech.edu

✉ Re: Former Oracle worker ... bogus e-mail ([RISKS-18.07](#))

"J.R.Valverde (jr)" <jrvalverde@samba.cnb.uam.es>

Fri, 26 Apr 1996 15:17:49 WET

I think PGN forgets a very important one:

10. Never accept to handle the account of some other person or having access to his/her computer.

The reason is obvious: should that person commit any crime s/he can always argue that since you had access to his/her account you could have forged or impersonated him/her. If that person is your boss and more powerful and reputed than you are, chances are s/he will be believed and you will charge with the responsibility for the crime.

Note: I'm not implying this could in any way whatsoever have happened in the Oracle case. But with computers it is now so easy to deny the authenticity of any document and imply it is a forgery that loading responsibilities on someone else's shoulders is trivial.

jr

✉ Re: Former Oracle worker ... bogus e-mail ([RISKS-18.07](#))

"John C. Rivard" <jcr@mcs.com>

Sat, 27 Apr 1996 16:40:48 -0500

Has the Assistant DA never heard of cellular modems?

John C. Rivard <http://www.mcs.net/~jcr/> jcr@mcs.com

✉ Re: Former Oracle worker ... bogus e-mail ([RISKS-18.07](#))

Simona Nass <simona@panix.com>

Sun, 28 Apr 1996 11:34:29 -0400 (EDT)

Adelyn Lee having Larry Ellison's password is significant. If she had his password, she may or may not have used it to send the e-mail. But as a RISKS matter, the technological evidence is not conclusive, even beyond some of the ways PGN mentioned.

For example, the cellphone records don't even have to be forged. Unless they checked all possible cellphone numbers in the area that he could have used, they can't rule out his having both his own cellphone and another line with a cellular modem. Or having had the e-mail sent via an at job or other automatic scheduled mechanism. Also, was the clock set to the same time for their computer and the cellphone records? Conceivably, he also could have had someone else with access do it (but allegations of conspiracy, like talk of black helicopters, don't do much to establish the credibility of a particular line of argument).

Since the technical evidence is not conclusive, it comes down to a credibility and bigger lawyers issue. I'm concerned about the precedent that may be established if judges rule on an issue while the parties have not explored all reasonable arguments about the technology. We'll

see what
happens with the perjury charge. -S.

Simona Nass simona@panix.com

[Clock synch problems also noted by tye@metronet.com (Tye McQueen). PGN]

⚡ Re: Former Oracle worker ... bogus e-mail ([RISKS-18.07](#))

<Steve_Kilbane@cegelecproj.co.uk>

Mon, 29 Apr 1996 09:33:06 +0100

Ah, this warms my heart, to know that we're learning lessons here: a person is charged with perjury, because computer records have shown that the computer records can't be trusted....

⚡ Coordination and Administration of the Internet: workshop CFP

"Tim Leshan" <LESHAN@ksgrsch.harvard.edu>

Mon, 29 Apr 1996 17:21:36 EST

Information Infrastructure Project
Harvard University
Commercial Internet Exchange Association (CIX)
Internet Society

COORDINATION AND ADMINISTRATION OF THE INTERNET
Workshop Announcement and Call for Papers

This is a first announcement and call for papers and proposals for a workshop to be held at the John F. Kennedy School of Government, Cambridge,

MA, USA, on September 8-10, 1996. The workshop will address issues in the international coordination and management of Internet operations. We are seeking papers which address the economic, organizational, legal and technical issues in migrating to internationally sanctioned, industry-supported processes and institutions. What should a fully internationalized Internet look like, and how do we get there from here?

Topics to be explored in the workshop and resulting publication include:

- policy and management issues concerning
 - network addresses
 - domain names
 - routing policy
 - settlements
 - interconnect points
 - intercontinental connectivity
 - quality of service standards

- legal and institutional structures for supporting core Internet functions

- institutions and policies needed to ensure the future scalability and extensibility of the Internet

- technical and implementation issues presented by heterogeneous national information policies

- the need for data in support of Internet planning, including issues of
 - how data should be collected and maintained

- coordination needed for the deployment of new technology

- international crisis management for the Internet

Although the Internet is already substantially privatized, certain essential functions -- notably the domain name registry, network number assignment, and the routing arbiter -- are still funded by the U.S. Government. Unlike the local telephone exchange, these integrative services are managed by third parties, contributing to an open competitive environment which has helped enable rapid growth of the Internet. Rapid growth, commercialization, and internationalization are putting stress on current institutions and procedures -- which are neither self-sustaining nor officially recognized at the international level. The National Science Foundation plans to phase out support for core administrative services and for international connections, just as it has withdrawn support for production-level backbone services. Conflicts over tradenames and number assignments suggest that international legitimacy is needed for domain name and network number management.

Beyond support for essential functions, there are many practical and policy issues where some greater degree of coordination or institutional leadership may be desirable. For example, how can the implementation of new technology and protocols be expedited? What common definitions and guidelines should exist to describe network performance? Should the functions performed by current Internet institutions (such as the Internic, RIPE, APNIC, and the IANA) be brought into a more robust international infrastructure, and if so, how? To what extent are multilateral peering arrangements and settlements

needed to encourage continued growth and competition in the Internet access industry?

The conference will engage scholars, practitioners and policy makers in examining and discussing these issue. It will bring together stake-holders, academics and individual leaders within and beyond the Internet community to help define the future institutional infrastructure of the Internet.

Workshop papers will be revised and edited following the workshop for publication by MIT Press as part of the Harvard Information Infrastructure Project series. Potential participants are encouraged to submit papers that can be developed and revised for publication (copyright assignment is not required). Please send an abstract by June 15, 1996, for review by the program committee.

Please direct papers, proposals, and requests for future mailings to:

James Keller
Information Infrastructure Project
Kennedy School of Government, Harvard University
79 JFK Street
Cambridge, MA 02138
617-496-4042; Fax: 617-495-5776
jkeller@harvard.edu

The Harvard Information Infrastructure Project is a project in the Science, Technology and Public Policy Program at the John F. Kennedy School of Government, with associated activities at the Kennedy School's Center for Business and Government and the Institute for Information

Technology Law and
Policy at Harvard Law School. This event and publication are
funded in part
by a grant from the National Science Foundation, Division of
Networking and
Communications Research and Infrastructure.



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 18: Issue 9

Weds 1 May 1996

Contents

- [Breaking Java security restrictions with Javascript](#)
[Stephen Anderson](#)
- [More on Java security](#)
[Peter Hughes](#)
- [Cambridge University systems hacked!](#)
[David Alexander](#)
- [File permissions 705](#)
[Mordechai T. Abzug](#)
- [Libel writ served by e-mail](#)
[Andrew Martin](#)
- [X-Image-URL e-mail header line](#)
[Andrew Dalke](#)
- [Internal e-mail addresses don't work](#)
[John Gilliver](#)
- [File your tax return on the Web!](#)
[Jakob Schiotz](#)
- [Australian court emulates Swedes](#)
[Ashley Robertson](#)
- [Re: Warning! My \[...\] let me \[act\]](#)
[Geoffrey Cooper](#)

- [Correction: The RISK of attributing error to malice](#)
[Paul R. Potts](#)
 - [Re: The RISK of attributing error to malice](#)
[Randal L. Schwartz](#)
 - [Odds of an accident for the Challenger](#)
[Michael Perelman](#)
 - [Children on the Internet: A Forum, Chicago, 18 May 1996](#)
[David E. Sorkin](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ **Breaking Java security restrictions with Javascript**

"Stephen.Anderson" <stephen@theplanet.net>
Wed, 1 May 1996 12:30:13 +0000 (GMT)

I'm unaware of whether this point has been raised: under Netscape 2.01 and Atlas, there is a hole in Java vs. Javascript security that allows an Applet to (amongst other things) contact a host other than that it was loaded from. As Netscape allows use of "javascript:" URLs, it is possible to construct a Javascript string in a Applet, then execute it by a call to `showDocument()`. This Javascript is **not** subject to the same security restrictions as the Applet.

There are only three immediate risks I can think of:

1. People can end up reading pages they didn't expect or have any wish to (though this is a risk with Javascript more than with Java, Java offers an extra layer of concealment)
2. On a related note, people can end up running Applets they didn't

expect to, from different hosts, and these Applets may be able to compromise security by communicating with each other.

3. Any Javascript security holes are also available to Java

Stephen Anderson, Planet Online : The White House, Melbourne Street, Leeds

LS2 7PS UK. +44 (0) 113 2345566 Stephen.Anderson@theplanet.net

🔥 More on Java security

Peter Hughes <peter@livepicture.com>

Wed, 1 May 1996 12:43:29 -0700

It seems to me that no end is in sight to the security holes in Java. In addition, I have been hearing that Java (and net access in general) will soon become more deeply integrated into desktop OSs. Just how bad could this get? Is there a way that uncontrolled or malicious Java applets could propagate themselves about the net? Examples:

- * A Java applet that runs server code, propagating itself from its own server?
- * An applet that inserts copies of itself into a server on a machine that is also used to run a browser?
- * An applet that runs compiler code, creating an application of the author's choosing on the target machine?
- * An applet that attaches itself to Java-enabled applications or their documents (a la Word macro virii), perhaps then using file sharing to propagate itself?

I can think of other scenarios that are not specific to executable

applets, such as the exploitation of security holes on the net. (The Morris worm is an example of such). Given how few users take security seriously (or understand its implications), how likely is an event that causes massive damage?

The folks that designed Java took all this and more into account, but the continuing bugs show that the propagation of executables of this type carries an inherent RISK. The community is to be commended for scrutinizing Java.

Pete

(I turned off Java, and I don't run Word 6)

⚡ Cambridge University systems hacked!

David Alexander <dave_ale@online.rednet.co.uk>

Mon, 29 Apr 1996 10:19:01 +0100

The following article was in Saturday 27th April (UK) Daily Mail newspaper:

Start>

Cambridge computer chaos as hacker hits secret files

A worldwide hunt has been launched for a computer hacker who accessed

sensitive research information at Cambridge University.

Confidential files

were broken into using the Internet. Now up to 10,000 academics and students

are being forced to alter their passwords as the university's

computer

experts try to plug the leak. Many of the files belong to top research scientists and contain commercial, academic and medical information.

Richard Stibbs, Director of computer science studies at the university said:

"The hacker could come from anywhere in the world. The potential damage to Cambridge University and beyond is enormous. Fortunately no files appeared to have been tampered with, but we are asking everyone to check very carefully."

The alarm was raised when a network security system which links universities

detected a rogue program in the Cambridge computer. The hacker is thought to

have gained access through the university's E-mail system, the Ethernet

[sic]. Experts are trying to trace when he broke into the system - which is

being replaced to prevent any similar lapses - and find out where the calls

came from. If caught, the culprit could face up to 5 years in jail.

<End

The usual RISKS apply, plus the risk of a panic replacement of the e-mail

system. How do you know that the replacement is more secure...at least you

know the strengths and weaknesses of the old one, and could probably patch it.

The other significant RISK is that of determining the location and identity

of the hacker. Speaking as an 'ex Cambridge man' I know the physical layout

and and structure of some of their systems. Until about 4 years

ago I could
have walked into one of several sites and access the system. In
the early
80s (ah, lost youth), several of my friends would use the
Engineering Dept
terminals for all-night MUD sessions over JANET. I only say
'until recently'
because I have moved 100 miles away. The same RISK must apply to
almost any
academic site, but somewhere like Cambridge, where the 'Town and
Gown' are
inextricably linked, with University and College buildings
spread right
across the city, make security a nightmare to enforce.

David Alexander, Camberley, England Dave_Alexander@online.
rednet.co.uk

🔥 File permissions 705

"Mordechai T. Abzug" <mabzug1@gl.umbc.edu>

Tue, 30 Apr 1996 00:22:29 -0400 (EDT)

Under IRIX 5.3 (and perhaps other Unix variants), if someone
'chmod's a file
or directory to allow world access but to deny group access (i.
e., 705),
then members of the user's group can't access the file. I don't
know why
this should be, but assuming it makes sense, I've found a way
around it,
even though I only belong to one group and can't 'newgrp': I
made a symbolic
link to the file and put it in my web directory. Many 'httpd's
(including
the one here) allow sym links to files/ directories outside the
user's web
directory, and many httpd runs as user nobody or guest.
Presto! Access to
the Mail directory of a friend who thought he was being quite

clever. Of course, I immediately showed him what I had done, and warned him to use 700, but I didn't have to. . .

Mordechai T. Abzug
<http://umbc.edu/~mabzug1> mabzug1@umbc.edu finger -l
mabzug1@gl.umbc.edu

⚡ Libel writ served by e-mail

Andrew Martin <apm@cs.uq.oz.au>
Wed, 1 May 1996 15:19:41 +1000 (EST)

[I suppose the only new risk here is that a court is seen to be believing some rather flimsy evidence.]

'The Electronic Telegraph' [Web Edition of Major UK Newspaper],
by Robert Uhlig, 1 May 1996

In a ground-breaking case, lawyers have used the Net to enforce a British court order overseas.

THE INTERNET has for the first time been used to serve a legal injunction outside the UK, arguably establishing a precedent allowing the global computer network to be used as a medium for distributing legal documents, in the same manner as a fax machine. The development could also spell an end to the freedom of speech enjoyed in hundreds of specialist news groups on the Internet, where users discuss a wide spectrum of matters ranging from the complexities of rival computer operating systems to libellous speculation on celebrities' sexual practices.

The media and entertainment law firm Schilling and Lom in London received threats, via e-mail, from an individual in Europe who claimed he was planning to disseminate libellous material about one of its clients over the Internet. "The e-mail contained the sender's two Internet addresses," said Jonathan Coad, a libel partner at the firm. "When an injunction was obtained against him, we persuaded Mr Justice Newman to grant us leave ex parte to serve an order via these e-mail addresses. "We have to prove that the defendant received the injunction, and used the 'return receipt' capability of e-mail to prove that the defendant had seen the injunction on his computer screen." Mr Coad added that the defendant also acknowledged separately that he had received the injunction.

[...another lawyer] pointed out that there was still doubt over which nation's laws applied if someone made a libellous statement on a global medium such as the Internet. "Courts will have to move with the times and there are a number of modern judges who are willing to make the move," he said.

✶ X-Image-URL e-mail header line

"Andrew Dalke" <dalke@ks.uiuc.edu>
Tue, 30 Apr 1996 00:47:41 -0500

I just received e-mail with a header line I have never seen before,

> X-Image-Url: <ftp://ftp.somewhere.else/pub/images/face.tiff>

It appears to replace the 'X-Face' header as the URL was an image of the sender's face.

The risks are similar to those of web browsers, but ones I hadn't expected from an e-mail message. Two are:

1) If the URL is accessed when I read my mail, by looking at the server logs the sender knows many things, including when I read my mail and the machine I use to do so.

Imagine if mail handled by an anonymous remailer did not strip out this header. The (supposedly) anonymous receiver checks e-mail, the mail reader contacts the originator's site, and the sender knows at least the machine the recipient uses, and probably has a good guess as to the identity.

2) Inappropriately designed mail readers might not offer a "Stop" button to stop the transfer of large images. If the mail message proper is displayed after the image is downloaded, it might take a long time to transfer the image, while the mail itself is just a few lines long.

Andrew Dalke dalke@ks.uiuc.edu

⚡ Internal e-mail addresses don't work

John Gilliver <john.gilliver@gecm.com>

Tue, 30 Apr 1996 15:50:44 +0100

In [RISKS 18.08](#) appeared:

: From: Andy Piper <andyp@wrath>
: The RISKS? Don't make assumptions about how your intended
audience will view

I was going to discuss this privately with the poster
(basically, although
it is to some extent a valid point, the practice of assuming
fixed-spacing
fonts for news - so that, for example, ^s come out right - is
quite
widespread); however, I noticed where I would be sending it. I
suspect this
is an address which works well internally, but would fail if I
tried to use
it.

I'm sure it is an old RISK, but obviously still needs
mentioning! {The
software I use at home [Turnpike] won't allow me to send to an
address
without an @ sign, and at least one dot after it, which must be
both
preceded and followed by at least one character, which would
have stopped me
sending the reply - but of course doesn't help anyone actually
wanting to
contact Andy. [Perhaps that was the intention (-:!!]}

J. P. Gilliver, GEC-Marconi Research Centre, GEC-Marconi Ltd,
GREAT BADDOW,
Essex, CM2 8HN, UK. +44 1245 242133 john.gilliver@gecm.com

[Yes, it is indeed an old risk, but still prevalent. I am
always astounded
at how many e-mail messages I cannot answer for this reason!
PGN]

[Plus, there are now more cases where there are large
internal networks,
so people may be increasingly under the impression that it

does work (as
they may spend some time e-mailing internally before
venturing into the
big wide world outside, which maybe they didn't as much
before). JPG]

🔥 File your tax return on the Web!

Jakob Schiotz <schiotz@nils.wustl.edu>

Fri, 26 Apr 1996 13:13:48 -0500

Last year I moved from Denmark to the United States, so I have just had the "pleasure" of filing my tax returns in two countries. This has made me appreciate the efforts the Danish authorities have made in recent years to make the process easier. Basically, almost everything they need to know has already been reported to the authorities by the employer(s), the bank etc. Then they send you a tax return form with the relevant numbers printed on them, and you are then supposed to check them, correct any wrong numbers (unlikely) and add any info they do not have (more likely).

This year they have gone a step further: you can call a specific number and use you touch tone phone to file, or you can file on the Web at <http://www.tastselv.toldskat.dk/> (in Danish). To file you need your CPR number (similar to the US social security number) and a 7-digit individual security code printed on the form. You can then fill out the form and submit it. If you make a mistake it can be corrected the same day, but if you discover it later you have to contact the local tax

authorities. This means that a manual override system is in place, IMHO a good thing.

I am not a lawyer, but there must be some legal RISKS here. If I try to cheat how are they going to prove that it was me? And even if they know, is filling a form on the Web has any legal value? I don't sign anything, can typing a code that presumably only I know be legally equivalent to signing a document?

A more worrying RISK is that somebody actually do mess with other peoples tax returns. They don't use encrypted transfers, so sniffing the security code should at least in theory be trivial. It may be easier to get the code by social engineering, especially if the victim has no experience with computers and passwords ("Hello, it's the tax department. Due to a computer error some of our records have been lost, would you please tell us the numbers printed on the front page of the tax return form we sent you?").

An even more scary situation is that someone actually breaks into the machine running the web server. The requirement that any corrections must be made the same day may actually be an example of good risk management. If the info is transferred from the web server to another computer, and if that other computer only accepts to amend a filed return on the same day the original was filed, then the damage from a hacker will be limited to the returns filed that day (although if that day is April 30, the last day to

file, the damage may still be considerable).

Finally, we should also consider the risk of typos. Whom do you trust the most to get the numbers right? Yourself, who will be directly affected by an error? The OCR program "reading" your handwriting? Or maybe the (tired) clerk that has to manually type in the numbers on the forms where the handwriting is too illegible? This is (IMHO) a point in favor of the type-it-yourself service.

Jakob Schiotz, Dept of Physics, Washington University, St. Louis, MO 63130
+1 (314) 935 4968 schiotz@howdy.wustl.edu Fax +1 (314) 935 6219

✶ Australian court emulates Swedes (re: Gong, [RISKS-18.06](#))

Ashley Robertson <ashley@cs.murdoch.edu.au>
Tue, 30 Apr 1996 11:07:43 -0800

A similar situation has occurred here in Western Australia. New parents of a baby boy were unable to give their child an ancestral name because of the accents on some of the characters. The name was not offensive or difficult to pronounce. The reason given was that the computer system of the Registry of Births and Deaths could not accept the name because it was not a standard ASCII character.

The solution was not as easy as removing the accents because that substantially changes the pronunciation of the name. The child remains unnamed!

Ashley Robertson, Murdoch University, WESTERN AUSTRALIA +(619)
360 2101
ashley@babbage.cs.murdoch.edu.au <http://www.cs.murdoch.edu.au/~ashley>

[I suppose you could try to name a child something like Ju-umlaut-rgen or He-aigu-le-grave-ne? (with or without the hyphens, according to your taste after rereading [RISKS-17.95](#)). PGN]

✉ Re: Warning! My [...] let me [act] (Bailey, [RISKS-18.03](#))

Geoffrey Cooper <geof@devices.com>
Thu, 18 Apr 1996 11:00:46 -0700

In [RISKS-18.03](#), Rob Bailey writes that a human operator is an intrinsic part of a system in which he or she operates. Therefore, the human operator must share the blame if the system fails.

This is true; Since the human is part of the system, the strengths and weaknesses of the human must be taken into account in "good" system design, just as must be done for any other system component.

In the original design of the manual typewriter, there was a problem with the operator hitting the keys too fast; this caused mechanical jams. The problem was solved by the addition of the QWERTY keyboard encoding, which slowed down the typist by alternating the key locations between his two hands. This is was an appropriate design for the human component, even if it does not excuse us from still using QWERTY today.

We bristle when the media leaps to blame the operator; we must similarly bristle if we leap to blame the machine. The RISKS we seek are in the combination of the two, when the interface with the machine confuses or confounds the operator and encourages mistakes.

For example, an airplane that is willing to touch down without the landing gear deployed is not necessarily a bad system design, since:

- the pilot has procedures to prevent this from happening, including licensing to ensure that the pilot understands these procedures.

- the pilot may need to land the plane in this way in an emergency.

Conversely, an autopilot that automatically limits the pilots steering requests to avoid damage to the airplane might indeed be a bad system design. The human component might correctly need to damage the airplane in a sharp turn in order to save the lives of the passengers.

- Geof Cooper, Compact Devices, Inc.

✂ Correction: The RISK of attributing error to malice ([RISKS-18.08](#))

Paul R. Potts <potts@cancer.med.umich.edu>
Tue, 30 Apr 1996 12:40:30 -0400

In the paragraph where I wrote:

>I haven't explained the duplicate copies on the remote machine
or why the
>message was seen earlier, but this isn't necessary in order to
convince me
>that this "forgery" was really an accident.

the text should have read "why the message wasn't seen earlier."
^^^^^

Since the mail program automatically opens windows holding
unsent outgoing
mail when it is launched, the question was why the staff member
did not see
the message the morning after it was written, when she fired up
her computer
and launched the mail program.

There are lots of possible reasons: maybe she hadn't really shut
down her
computer and didn't re-launch the mail program the next morning,
or maybe
she simply didn't notice the mail message, or maybe the mail
program didn't
open the window for some reason.

I jumped to the conclusion that perhaps the file's creation date
had been
faked by resetting the Macintosh system clock, obviously failing
to apply
Occam's razor to the various hypotheses. I'm confident that our
moderator
can come up with an appropriate pun here, perhaps something
about shooting
the mail-message(r) or a close shave that cuts both ways :)

"Paul R. Potts" Technical Lead - Health Media Research Lab
University of Michigan Comprehensive Cancer Center potts@cancer.
med.umich.edu

⚡ Re: The RISK of attributing error to malice (Potts, [RISKS-18.08](#))

"Randal L. Schwartz" <merlyn@teleport.com>

Tue, 30 Apr 1996 08:14:54 -0700 (PDT)

And such an unfounded witch-hunt can even further lead to criminal convictions, as it did in my case. For details, see the website <http://www.lightlink.com/fors/>. If you are web-challenged, you can get the executive summary by writing to my reply-bot at fund@stonehenge.com (the content will be mostly ignored).

I urge everyone with system administration responsibilities to be aware of this case, and to share the information with others.

Randal L. Schwartz / Stonehenge Consulting Services (503)777-0095
<merlyn@stonehenge.com> Snail: (Call) PGP-Key: (finger
merlyn@ora.com)

⚡ Odds of an accident for the Challenger

Michael Perelman <michael@ecst.CSUCHICO.EDU>

26 Apr 1996 01:58:33 GMT

I have heard that just before the Challenger flight, NASA issued a reports of the odds of an accident. Does anybody know of a source? What were the odds?

Michael Perelman, Economics Department, California State University
Chico, CA. 95929 michael@ecst.csuchico.edu

⚡ Children on the Internet: A Forum, Chicago, 18 May 1996

"David E. Sorkin" <7SORKIN@jmls.edu>

Tue, 30 Apr 1996 20:07:19 CST

The John Marshall Law School Center for Informatics Law, in association with the Illinois Privacy Council, announces the following conference:

CHILDREN ON THE INTERNET: A FORUM FOR PARENTS AND EDUCATORS.
Saturday, May 18, 1996, 8:30 am-5:30 pm, at The John Marshall Law School, 315 South Plymouth Court, Chicago, Illinois.

The purpose of The Forum is to explore the benefits of the Internet and online services and to learn about risks as well, so that informed parents and educators can cooperate with service providers so as to enjoy the advantages of the Internet while avoiding the negatives. Panelists will demonstrate Internet resources available for children; will discuss the potential for commercial manipulation of children, invasions of privacy, access to objectionable materials, and other risks; and will suggest appropriate roles and responsibilities of parents, educators, and institutions in minimizing these risks.

The registration fee of \$40 includes continental breakfast, lunch, and conference materials. Registration deadline: May 13, 1996. Space is limited.

For more information, call the Center for Informatics Law at (312) 987-1419, or e-mail privacy@jmls.edu. Information about the Forum is also available on the World Wide Web at <http://www.jmls.edu/conf/ipcforum/>.

-- David E. Sorkin (7sorkin@jmls.edu)
-- Associate Director, Center for Informatics Law, The John Marshall Law School

[I wonder if there are any three-generation families of RISKS readers? I know there are a bunch of two-generation families. PGN]

⚡ UNABRIDGED Info on RISKS (comp.risks), subscriptions, etc.

<RISKS-request@csl.sri.com>

1 April 1996 (no fooling!) (LAST-MODIFIED)

The RISKS Forum is a moderated digest. Its USENET equivalent is comp.risks.

Undigestifiers are available throughout the Internet, but not from RISKS.

SUBSCRIPTIONS: PLEASE read RISKS as a newsgroup (comp.risks or equivalent) on

your system, if possible and convenient for you. BITNET folks may use a

LISTSERV (e.g., LISTSERV@UGA): SUBSCRIBE RISKS or UNSUBSCRIBE RISKS. U.S.

users on .mil or .gov domains should contact <risks-request@pica.army.mil>

(Dennis Rears <drears@pica.army.mil>). UK subscribers please contact

<Lindsay.Marshall@newcastle.ac.uk>. Local redistribution services are

provided at many other sites as well. Check FIRST with your local system or

netnews wizards. If that does not work, THEN please send requests to

the newly automated <risks-request@csl.sri.com>, with first text line

SUBSCRIBE or UNSUBSCRIBE

[with option of E-mail address if not the same as FROM: on the same line].

INFO

gets you this file.

HELP

gives instructions on using the Majordomo listserver in other

ways,

although not all are yet implemented for RISKS.

CONTRIBUTIONS: to risks@csl.sri.com, with appropriate, substantive Subject:

line, otherwise they may be ignored. Must be relevant, sound, in good taste,

objective, cogent, coherent, concise, nonrepetitious, and without caveats

on distribution. By submitting an item that is accepted for publication in

RISKS, the author grants permission for unlimited noncommercial public

distribution and redistribution in electronic and print form.

Diversity of content is welcome, but not personal attacks.

PLEASE DO

NOT INCLUDE ENTIRE PREVIOUS MESSAGES in responses.

Contributions will not be

ACKed; the load is too great; if you feel neglected, send a follow-up message.

****PLEASE**** include your name & legitimate Internet FROM: address,

especially from .UUCP and .BITNET folks. Anonymized mail is not accepted.

ALL CONTRIBUTIONS CONSIDERED AS PERSONAL COMMENTS; USUAL DISCLAIMERS APPLY.

Particularly relevant contributions may be adapted for the RISKS sections

of issues of ACM SIGSOFT Software Engineering Notes or SIGSAC Review.

* Submissions: By submitting an item that is accepted for publication

in RISKS, the author grants permission for unlimited public distribution

and redistribution in electronic or other form.

* Reuse: Blanket permission is hereby granted for reuse of all materials

in RISKS, under the following conditions. All redistributed items must

include the Risks-Forum masthead line. All reuse must be accompanied by

the following statement:

Reused without explicit authorization under blanket permission granted for all Risks-Forum Digest materials. The author(s), the RISKS moderator, and the ACM have no connection with this reuse.

As a courtesy, reusers of individual items (as opposed to forwardings of entire issues) should notify the authors, and should pay particular attention to any subsequent corrections.

RISKS can also be read on the web at URL <http://catless.ncl.ac.uk/Risks>

Individual issues can be accessed using a URL of the form <http://catless.ncl.ac.uk/Risks/VL.IS.html> [yes, VL = volume, IS= issue]

(Please report any format errors to Lindsay.Marshall@newcastle.ac.uk)

RISKS ARCHIVES: <ftp://unix.sri.com/risks> if your browser accepts URLs, or

```
ftp unix.sri.com<CR>login anonymous<CR>[YourNetAddress]<CR>
cd risks<CR> or cwd risks<CR>, depending on your particular
FTP;
```

Issue J of volume 18 is in that directory: "get risks-18.J<CR>". For issues of earlier volumes, "get I/risks-I.J<CR>" (where I=1 to 17, J always TWO digits) for Vol I Issue j. Vol I summaries in J=00, in both main directory

and I subdirectory; "bye<CR>" I and J are dummy variables here. REMEMBER,

Unix is case sensitive; file names are lower-case only.

<CR>=CarriageReturn;

FTP.SRI.COM = [128.18.30.66]; FTPs may differ; Unix prompts for username and

password. Also ftp bitftp@pucc.Princeton.EDU. WAIS repository exists at

server.wais.com [192.216.46.98], with DB=RISK (E-mail info@wais.com for info)

or visit the web wais URL <http://www.wais.com/> .

Management Analytics Searcher Services (1st item) under <http://all.net:8080/>

also contains RISKS search services, courtesy of Fred Cohen. Use wisely.

The ftp.sri.com site risks directory also contains the most recent PostScript copy of PGN's comprehensive historical summary of one liners: get illustrative.PS

PRIVACY DIGESTS:

* The PRIVACY Forum is run by Lauren Weinstein, with some support from the ACM Committee on Computers and Public Policy. He manages it as a rather selectively moderated digest, somewhat akin to RISKS; it spans the full range of both technological and non-technological privacy-related issues (with an emphasis on the former). For information regarding the PRIVACY Forum, please send the exact line:

information privacy

as the first text in the BODY of a message to:

privacy-request@vortex.com

You will receive a response from an automated listserv system. To submit contributions, send to "privacy@vortex.com".

Information and materials relating to the PRIVACY Forum may also be obtained from the PRIVACY Forum Archive via ftp to "ftp.vortex.com", gopher at "gopher.vortex.com", and World Wide Web via: "<http://www.vortex.com>". Full keyword searching of the PRIVACY Forum Archive is available through the World Wide Web access address.

* The Computer PRIVACY Digest (CPD) (formerly the Telecom Privacy digest) is

run by Leonard P. Levine. It is gatewayed to the USENET newsgroup

comp.society.privacy. It is a relatively open (i.e., less tightly moderated)

forum, and was established to provide a forum for discussion on the

effect of technology on privacy. All too often technology is way ahead of

the law and society as it presents us with new devices and applications.

Technology can enhance and detract from privacy. Submissions should go to

comp-privacy@uwm.edu and administrative requests to comp-privacy-request@uwm.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 18: Issue 10

Tuesday 7 May 1996

Contents

- [The Cali and Puerto Plata B757 Crashes](#)
[Peter Ladkin](#)
- [Telephone accounting](#)
[Warrick Jackes](#)
- [DOs and DON'Ts: A Perversity of Owner's Manuals](#)
[Ken Knowlton](#)
- [30% of the births in California](#)
[Bob Frankston](#)
- ["Survey Finds Computers Under Siege"](#)
[Peter G. Neumann](#)
- [RISKS posting leads to e-mail attack!](#)
[Martyn Thomas](#)
- [Denial of service made easy....](#)
[David Leshner](#)
- [ACLU Post-Trial Brief on the Web Site](#)
[Ann Beeson](#)
- [Re: Cambridge University systems hacked!](#)
[Stephen Early](#)
- [Re: AOL censors British town's name!](#)
[Peter Miller](#)

● [Re: Odds of an accident for the Challenger](#)

[Gareth McCaughan](#)

[Pete Mellor](#)

[Paul Green](#)

[Dani Eder](#)

● [Info on RISKS \(comp.risks\)](#)

✶ The Cali and Puerto Plata B757 Crashes

<ladkin@TechFak.Uni-Bielefeld.DE>

Tue, 7 May 1996 23:29:07 +0200

On December 20, 1995, American Airlines flight 965 (AA965), a B757-223

serial number N651AA, crashed into mountains on approach to Cali, Colombia.

This was the first B757 fatal accident in a decade and a half of service,

and I believe the first jet accident for AA in about the same length of time.

On February 6, 1996, a B757 of Birgenair, registration TC-GEN, crashed

into the ocean off Puerto Plata, Dominican Republic, shortly after takeoff.

This was the second fatal B757 accident.

The US National Transportation Safety Board is 'participating fully' in each of the investigations. Statements and documents concerning the accidents

released by the Columbian and Dominican Republic agencies are available from

the NTSB. Statements on Cali were released on 28 Dec 1995 and Feb 15 1996,

and the 'docket' (containing the factual reports of the 'specialty groups'

of investigators) has been released recently. Statements on the Puerto Plata

accident were released Feb 7, Mar 1 and Mar 18 1996. Final

reports for
neither are yet available.

Contrary to the impression given by some recent articles in the non-specialist press, neither findings nor causes nor causal factors have yet been officially determined in either investigation. However, the factual reports so far indicate to me that the human-computer interface could be involved in both accident sequences. These airplanes have a safety record amongst the best of any type in regular airline use - many B757 and B767 aircraft have been flying for a decade and a half in the fleets of airlines all over the world, and there have only been three fatal accidents (the first, to a Lauda Air B767, is thought to have been due to an unrecoverable technical failure alone). After 16 years of exemplary safe use, one should therefore not be too hasty to 'blame the computer' or its interface. Here are some comments on both accidents.

Cali:

Happened on approach to the airport, which is aligned along a relatively narrow valley with high mountains to either side. Because of benign weather conditions, the pilots were offered a 'straight in' approach (to land in the direction they were flying) rather than to fly beyond, turn, and land in the opposite direction (the more usual procedure). They were not familiar with the 'new' approach. During the approach procedures, the pilots were confused about exactly where they were in relation to the arrival procedure charts. They had passed a specific radio beacon (VOR) called Tulua,

which is the start of the arrival procedure. It seems that they were not aware that they had done so, entered this fix into the Flight Management Computer (FMC), and didn't immediately notice that the aircraft had begun to turn back to the Tulua VOR. This turn began a quick sequence of events that led to impact with a mountain (a CFIT, Controlled Flight Into Terrain accident) about 3,000ft below the summit. A Ground Proximity Warning System warning sounded about 9 seconds before impact, initiated recovery procedures (full power, maximum angle of climb, retract any draggy control surfaces that are deployed). The crew didn't retract the speed brakes (manually controlled), which is a necessary part of the escape procedure.

The actual manoeuvres that led to impact were that of turning towards a specified VOR, and turning towards a specified heading. Both were initiated by the crew. The former was apparently accomplished with the FMS, the latter with the autopilot. Small airplanes such as my Piper Archer have autopilots capable of such manoeuvres. The pilot flying must command either, as happened at Cali. However, the more sophisticated FMC requires more attention than a simple autopilot when entering fixes, and investigators are paying attention to the role the FMC-pilot interaction played.

The question that arises is what exactly played a causal role. There is a known HCI phenomenon that when something is 'not right', it takes more time and attention to 'debug' the situation when more sophisticated

devices are involved than when simpler ones are being used. However, there were also other, human, procedural problems. The December 28 statement noted that there was no indication of descent checklist procedures being performed by the crew, and no indication of an arrival or approach procedures briefing. Also, it is a basic rule of flying that you know where you are at all times. These pilots didn't, at a crucial phase of flight, even though they had reputations for conscientiousness (see the Operational Factors/ Human Performance factual report).

Their confusion may have been aided also by some of the pilot-controller discourse about the route for which they were cleared. (However, there was no evidence of 'language difficulty', as this is usually understood.)

Puerto Plata:

The captain's airspeed indicator (ASI) was observed to be failed on takeoff. This is not an event that requires emergency handling. The captain asked the copilot to call out the significant airspeeds for takeoff (called V1 and V2, also normal procedure) and took off as normal. He then called for the center autopilot to be switched on. His own airspeed indicator showed higher and higher airspeeds as the aircraft climbed, even though the actual airspeed of the aircraft (as recorded by ground radar) was much lower. The first officer observed that his ASI showed marked decrease in airspeed, and the pilots became confused over which ASIs were failed (the

captain thought at one point that they'd both failed). The aircraft apparently stalled and the pilots did not succeed in recovering before hitting the ocean.

The DR/NTSB factual statement noted that the behavior of the aircraft was consistent with the captain's pitot being blocked. The airplane had been sitting on the ground for many days in the tropics without the pitots being covered (there is no procedural requirement for this, but pilots and mechanics all know that insects love pitots). The pitot is a tube facing into the airstream receiving air pressure facing in the direction of flight, and a related static port receives (roughly) ambient air pressure. The difference between the two is used to drive the ASIs in all aircraft. If the pitot is blocked, then pitot pressure remains roughly constant and ambient air pressure decreases as the aircraft climbs, leading to greater difference between pitot pressure and static pressure, and thus to greater 'indicated' airspeed on the ASI.

The copilot has a separate pitot-static system. The pitot-static readings on the B757 are fed into the left (for the captain's system) and right (for the copilot's) Air Data Computers, and thence to the CRT display instruments for the respective positions. There is a third pitot-static system that is purely mechanical (and therefore 'traditional'). Normally, pilots of all airplanes are also trained to use 'alternative source' if a pitot-static system fails. 'Alternative source' on the B757 is to switch the

displays so that the captain's ASI reads from the right ADC and the first officer's from the left ADC. Also, the 'glass' ASIs should be checked against the mechanical 'backup'. There is no evidence that either 'alternate source' was used during the accident flight, or that either instrument was checked against the backup, even when the captain falsely thought that both his and the first officer's ASIs had failed.

David Learmount asserted in Flight International (27 Mar - 2 April) that the central autopilot gets its data from 'the' ADC. He must have meant to say from the *left* (captain's) ADC. Supposing this is the case, the autopilot would react to the (false) increasing airspeed indication by raising the nose, to attempt to reduce 'airspeed'. Continuing to do so, since the false 'airspeed' continued to increase with increasing altitude, the airplane would radically lose (real) airspeed, and eventually stall, which appears to be what happened. I have not yet been able to verify Learmount's (modified) assertion with the NTSB or Boeing engineers. The question arises, why would the captain switch on the center autopilot if his ASI had failed and he knew it got its data from the same ADC? Anecdotal information (a colleague with access to a B757 operations manual, another who is a B757 pilot) suggests that this might not be information that one could expect to be at the front of every B757 pilot's mind. These two situations (center AP gets data from left ADC; this information not in the mental foreground when dealing with

ASI problems) may thus have played a causal role in the accident. (I emphasise again that I have not yet confirmed either situation.) This could be categorised as an HCI issue. As at Cali, there were other apparent procedural failures: failure to switch to 'alternate source'; failure to check against the standby mechanical instrument. Performance of either would have avoided the accident: as Learmount says, the pilots lost control of a flyable airplane.

Further Commentary:

Maybe one can see in these accidents two known and often-observed HCI effects of automation, which I shall call Complacency and Complexity. The Complacency effect is that use of (normally reliable) automation can lead to reduced awareness of the state of the system. The Complexity effect is that increased automation makes some straightforward tasks more complex and interdependent. The effects are distinct, but both have the consequence that it becomes harder to figure out what's going on when something is wrong. As a discussion point, let me propose that the greater role at Cali seems to have been played by the Complacency effect, with some Complexity effect; and that at Puerto Plata by the Complexity effect alone. For the answers, we'll have to wait until the final reports.

Finally, I don't regard either accident as giving grounds for concern about the role of automation in itself. But the reports might yield insights into and improvements to the procedures for dealing with certain

forms of
automation. One always hopes to learn from the tragedies.

The text of the official statements referred to above, as well as other pertinent documents, may be found in the sections on these accidents in the hypertext Compendium 'Computer-Related Incidents and Accidents to Commercial Airplanes' under <http://www.techfak.uni-bielefeld.de/~ladkin/>

Peter Ladkin

✶ Telephone accounting

Warrick Jackes <wjackses@cit.gu.edu.au>
Tue, 7 May 1996 20:03:49 +1000 (EST)

* Cutting: "Sunday Mail (Brisbane)", Sunday, the 14th April 1996, page 12:

A Brisbane bloke was stunned to discover on his latest phone bill an amount of nearly \$900 for a call of more than 10 hours duration to the Solomon Islands. The bloke does occasionally call the Solomons and does admit to being a bit of a yakker [talk the doors off a barn]. But for 10 hours? Query with Telstra [read as Bell Australia] brought the testy advice that he must have forgotten to hang up his receiver. The bloke pointed out that this theory was flawed by Telstra's own bill that showed that he'd used the same phone to call Melbourne (Australia) only 11 minutes after the start of the call to the Solomons.

* Cutting: "Sunday Mail (Brisbane)", Sunday, the 21st April 1996, page 12:

This case apparently stirred Telstra into prompt action. By Monday, 15 April, the matter had been "investigated" and the charge waived.

Warrick JACKES, 52 Hamilton Road, MOOROOKA, Q. 4105 AUSTRALIA
+61 411 18 55 68 wjackes@cit.gu.edu.au

[Otherwise, he would have been a Gofer-Bloke. PGN]

✶ DOs and DON'Ts: A Perversity of Owner's Manuals

Ken Knowlton <KCKnowlton@aol.com>

Tue, 7 May 1996 17:38:58 -0400

Letter-to-the-editor of *The New York Times* Magazine section, 5 May 1996,
quoted in full:

> James Gleick's 'manual Labor' (Fast Forward, April 7) touched a
> long-tender sore spot with me. For example, the manual that
came
> with a car I bought not long ago contained no fewer than 31
Cautions,
> 32 Warnings, 28 Do Nots and 2 Nevers. (I never did discover
the
> difference between a Do Not and a Never). My favorite was
this:
> `Do not open sun roof when car is covered with snow.'
> Robert L. Wolke, Pittsburgh"

So much stuff to remember, but so few reasons. Wouldn't it be a
lot easier
to remember (or forever dismiss) such advisories if we knew the
reasons, and
had a structure to hang them on? Suppose I'm wedged between two
trucks, the

car is on fire, but there's still some snow on the roof. Should I try to get out through the sun roof? Do I risk only the obvious (some snow down my neck) -- or a death worse than by fire? Maybe best to wait til the snow has melted and hope that by then I'm not already fried? After all, if they've taken such pains to tell me something, then more than the obvious risk must be involved -- because if it were only the obvious, it wouldn't need to have been stated, right?

✶ 30% of the births in California

<Bob_Frankston@frankston.com>

Sat, 4 May 1996 07:25 -0400

I heard on the radio today that a state legislator wondered why she was getting literature aimed at single parents. Investigating, she discovered that the state didn't record the marital status on birth records. Instead, they assumed that if the parents' last names were not the same, they were both single!

And these are the kind of "statistics" on which we base public policy!

In thinking about the 30% of the California mothers who are thereby supposedly single, I realize that the issue is deeper than bad methodology; it is the reason why such numbers become important. Much public policy is driven by numbers. The CPI (Consumer Price Index) is a more

pervasive

example. It reflects something or another but what is less important than that there be a way to keep score.

Lest we blame the government, remember how much business policy is also "by the numbers" -- numbers that aren't necessarily accurate. In one case a very large company assigned a programmer to assure consistency in the numbers they had gathered from the field, which were the basis for billions of dollars of corporate decision making. He discovered that after attempting to clean up the data that it was essentially pure noise by the time it was massaged.

More obvious and more explicit are the "sweep" numbers used by television stations. Someone more involved in the specifics should provide the details but apparently the advertising rates are set by tallying the viewing during designated weeks. The problem is that everyone knows which weeks they are and therefore create special shows to cook the numbers. Is there a better system?? Perhaps not.

This is, of course, a risk of technology in that we have much better tools to gather numbers than we did in the past. But we also need some agreed to rules even if they are perverse. Interestingly, these numbers might assure some degree of fairness by being so noisy that it is hard to predict their outcome using inside knowledge. But, maybe I'm just getting too cynical. Or pragmatic?

✦ "Survey Finds Computers Under Siege"

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

Tue, 7 May 96 17:50:27 PDT

Much as I dislike statistics about ``computer crimes'', this might at least be worth noting for the RISKS archives.

Jon Swartz, writing in the **San Francisco Chronicle**, 7 May 1996, p. C1, summarized the conclusions of a survey just released by the Computer Security Institute and the FBI's International Computer Crime Squad. 41% of the respondents admitted to electronic intrusions or unauthorized probes of their systems by disgruntled employees or competitors in the past year, and roughly half of those involved insiders. The Internet has become a "prime source" of such activities. 20% said they did not know whether they had been invaded; and nearly 75% of those said they would not report incidents because of fear of negative publicity. Medical and financial institutions were particularly prone to data manipulations. (There were 428 respondents out of almost 5000 queried.)

One of the biggest problems in justifying the need for computer security has always been that many organizations and individuals appear not to have been compromised. The 75% figure is perhaps the most interesting.

⚡ RISKS posting leads to e-mail attack!

Martyn Thomas <mct@praxis.co.uk>

Tue, 7 May 1996 18:41:47 +0100 (BST)

This morning, I started to receive e-mails accusing me of forcing a Swedish band called Ace of Base to leave Sweden for ever. The e-mails continue to arrive - some are very abusive. I have never heard of Ace of Base! (AoB)

Some detective work later, I discover the story: Scandinavian Airlines (SAS) have reviewed Ace of Base in their in-flight magazine (apparently) and said that they prove that musical ability is not a requirement for Swedish bands (I paraphrase).

An AoB fan has produced a Web page (<http://www.ultranet.com/~wurther/opmdv.htm>) that gives the story and invites readers to send their views by e-mail to a "senior SAS official"; he then gives **my** e-mail address!

Why does he do this? I'm guessing, but an Altavista search for my e-mail address turns up Jan-Erik Andelin's MD80 Accidents Pages (<http://www.clinet.fi/~andelin/md80acsk.htm>) containing a copy of a report I posted to Risks in November 1993, quoting a Flight International report on the Dec 1991 crash of an SAS MD-81! So I guess that "Wurther" searched for SAS, found this page, assumed I must be an SAS official, and added me to his list of hate targets!

I've mailed him and his webmaster, so far with no effect.

Martyn Thomas, Praxis plc, 20 Manvers Street, Bath BA1 1PX UK.
+44-1225-444700. mct@praxis.co.uk Fax: +44-1225-465205

⚡ Denial of service made easy....

David Leshar <wb8foz@nrk.com>

Fri, 3 May 1996 14:13:14 -0400 (EDT)

re: X-URL: <http://www.bell-atl.com/college/>

Bell Atlantic is making it easy for students to disconnect service. Of course, they are also making it easy for OTHERS to disconnect service for you, and exposing the information you provide to anyone in between....

⚡ ACLU Post-Trial Brief on the Web Site

Ann Beeson <beeson@pipeline.com>

Wed, 1 May 1996 12:39:26 -0400

Folks following the ACLU v. Reno/ALA v. DOJ case may want to check out our post-trial brief, filed this past Monday and now available from our home page at <http://www.aclu.org> .

We'll also be posting our joint (ACLU/ALA) 200-page "Findings of Fact" shortly. That document neatly reorganizes all of the evidence presented at the hearing.

The next and final step in the case is oral argument, scheduled for Friday,

May 10th, at 9:30 a.m. in Philly.

Ann Beeson
Staff Counsel, _ACLU v. Reno_
American Civil Liberties Union
132 W. 43rd St.
NY, NY 10036
212-944-9800 x788

[Courtesy of Audrie Krause, Executive Director, CPSR, P.O. Box
717 Palo Alto
CA 94302 (415) 322-3778 akrause@cpsr.org * Web: <http://cpsr.org/home.html>]

⚡ Re: Cambridge University systems hacked! ([RISKS-18.09](#))

Stephen Early <sde1000@chiark.chu.cam.ac.uk>
Thu, 2 May 1996 11:19:11 +0100 (BST)

Another two risks demonstrated here are:

Summarisation of technical information by people who do not understand it
- a reporter in this case, but the risk probably applies elsewhere

Believing what newspapers print.

The story printed in the newspaper bears only a passing resemblance to the real incident. What actually happened was that a packet sniffer was found running on a machine on the subnet that connects the central Unix service, mail server, and so on. Everyone who uses these systems was required to change passwords. The e-mail system has not been replaced, and I've no idea how this detail got into the article.

Steve Early sde1000@cam.ac.uk

⚡ Re: AOL censors British town's name! (Overy, [RISKS-18.08](#))

Peter Miller <pmiller@bmr.gov.au>

Mon, 6 May 96 11:39:30 EST

> 1) Use PGP.

This does not help. What if the output of PGP encryption innocently contains the byte sequence 0x63 0x75 0x6E 0x74? Being gibberish, you didn't check - but the computer may, and censor it. There are similar problems with uuencode, rot13, etc. Sigh!

Peter Miller pmiller@agso.gov.au uunet!munari!agso.gov.au!
pmiller

[Sigh-bernetics caught in a sigh-clone? Sigh-onara!
Imagine being tossed in jail because your encrypted
message just happened to trigger a filter! PGN]

⚡ Re: Odds of an accident for the Challenger (Perelman, [RISKS-18.09](#))

Gareth McCaughan <G.J.McCaughan@pmms.cam.ac.uk>

Thu, 2 May 96 11:03 BST

I don't know about any public announcement, but in Richard Feynman's "What do you care what other people think?" there is an extended account of his

part in the investigation of the Challenger disaster, including quite a lot about the odds quoted within NASA for various kinds of failure, and their (often tenuous) relation to reality.

I'm afraid I don't remember any of the figures, but they were wildly overoptimistic. One interesting thing was that when Feynman talked to the engineers who actually worked on the shuttle components, they gave pretty good estimates for things; but somehow, as information propagated up the management structure, it got fudged. (Cf. the entry in the Jargon File under "SNAFU principle".)

Gareth McCaughan Dept. of Pure Mathematics & Mathematical Statistics,
gjml1@pmms.cam.ac.uk Cambridge University, England.

[Re: Odds of an accident for the Challenger \(Perelman, RISKS-18.09\)](#)

Pete Mellor <pm@csr.city.ac.uk>
Thu, 2 May 96 11:05:20 BST

[Referring to Richard P.Feynmann: "What Do You Care What Other People Think?", Unwin Hyman Ltd. (London), 1988, ISBN 0-04-440341-0 (first published in USA in 1988 by W.W.Norton & Company Inc.) Chapter "Fantastic Figures" pp 177-188.]

> What were the odds?

10⁻⁵ (i.e., 1 in 100,000) was NASA's "official" figure.

Feynman quotes the range safety officer at Kennedy as having arrived privately at an estimate of 1 in 100 (based on observation that 4% of unmanned flights failed, and an optimistic assumption that manned craft must be safer).

Peter Mellor, Centre for Software Reliability, City University, Northampton Square, London EC1V 0HB, UK. Tel: +44 (171) 477-8422 p. mellor@csr.city.ac.uk

[Also commented on by
smurf@noris.de (Matthias Urlichs).
"Ratzka Wolfgang Dr." <ratzka@braun0.HRZ.Uni-Marburg.DE>
Roy Murphy <murphy@panix.com>
PGN]

✈ Re: Odds of an accident for the Challenger (Perelman, [RISKS-18.09](#))

<Paul_Green@vos.stratus.com>
Tue, 7 May 96 12:24 EDT

I have Volume I of the Report of the Presidential Commission on the Space Shuttle Challenger Accident (U.S. Gov't Printing Office, June 6th, 1986). There are 5 volumes; Volume I is the summary and has 256 pages. It is well-written, easy-to-read, and remarkably free of technobabble. Any large library should have it; some of it is also online at <A HREF="<http://www.ksc.nasa.gov/shuttle/missions/51-1/docs/rogers-commission/table-of-contents.html>">Rogers Commission Report .

Nowhere in this volume could I find a reference to the numerical odds

of a shuttle accident. There are many statements that recognize that there are risks that cannot be totally eliminated. Conceivably, there might be a calculation of the odds in one of the other volumes of the report. According to [NASA Press Release](http://spacelink.msfc.nasa.gov/NASA.Projects/Human.Space.Flight/Shuttle/Shuttle.Program.Changes.Since.1986) there has been 1 failure in 74 flights (thru January 1996), for a reliability of 0.986. (I asked a web index tool to find references to "odds of a space shuttle accident" to find these documents.)

Personally, I believe that every practicing engineer, and every manager in an engineering organization, should read this report regularly. It is both enlightening and sobering on the difficulties of building reliable, complex systems in the real world.

The accident was caused by "known problems" in a faulty design. The attempted resolution of the problems was poorly executed and poorly managed. Safety concerns were not escalated up the management chain. Known problems were dismissed as "still within limits". Launch constraints were waived at the expense of safety. Management reversed the position of its own engineers. All of this came out at the time, but perhaps some people who were not around at the time have not heard about it. I urge everyone to read it.

Paul Green, Senior Technical Consultant, Stratus Computer, Inc.,
Marlboro, MA
01752 Paul_Green@stratus.com +1 508-460-2557 FAX: +1 508-460-0397

✉ Re: Odds of an accident for the Challenger (Perelman, [RISKS-18.09](#))

Dani Eder <ederd@bcstec.ca.boeing.com>

Thu, 2 May 1996 17:11:50 GMT

I have not seen that report, but in the late 1980's, when I was working on Shuttle-derived launch vehicle studies, we did an in-house assessment assuming the fixes post-Challenger were made correctly. We got a figure of 1 in 70 per launch of losing an Orbiter, and 1 in 100 per launch in losing the crew. The difference in the two figures is because you can have a landing that the crew can walk away from, but the landing was hard enough to overstress the Orbiter structure, so that you have to write off the vehicle.

Dani Eder

[Further comments from
Ann_Holt@ftdetrck-ccmail.army.mil. 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 18: Issue 11

Monday 13 May 1996

Contents

- [Massive failure of Washington DC traffic lights](#)
[Jeremy J Epstein](#)
 - [Computer Error in phone bills](#)
[Mike Schwartz](#)
 - [Reactivating Windows95 Screen Savers](#)
[Mich Kabay](#)
 - [Re: AOL censors British town's name!](#)
[Xcott Craver](#)
[Dave Horsfall](#)
 - [Re: Odds of an accident for the Challenger](#)
[Hal Lewis](#)
[Jordin T. Kare](#)
 - [Internet in danger](#)
[Patrick Robin via Gordon Peterson](#)
[Bill Frantz](#)
[and Martin Minow](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ Massive failure of Washington DC traffic lights

JEREMY J EPSTEIN <JEPSTEIN@mail.cordant.com>

Fri, 10 May 1996 09:19:35 -0500

According to the 9 May 1996 **Washington Post**, most traffic lights in downtown Washington D.C. went onto their weekend pattern (typical: 15 seconds of green per light), rather than their rush hour pattern (typical: 50 seconds of green per light). This occurred during the Wednesday (8 May) morning rush hour. The problem was reportedly caused by a new version of software installed in the central system that controls all of the traffic lights, providing timing (so lights turn green in sequence). The result was mile-long traffic jams. One woman reported that her 35-minute commute turned into 75 minutes, due to the overloaded streets.

By the afternoon rush hour, the software glitch had been "fixed". It wasn't clear whether that meant they reloaded the old software or fixed the bug.

Some might consider this a risk of computer controlled systems, and others might consider it a substantial increase in the nation's productivity: think of all the lawyers and congresscritters who couldn't get to work!

⚡ Computer Error in phone bills

Mike Schwartz, Phoenix Chapter ACM; +1.602.561.1223 <schwartz@ACM.ORG>

Thu, 09 May 1996 20:00:28 +0000 (GMT)

I thought this might be of interest not so much because it made

a big splash
in the news recently here in the Phoenix area (both print and
broadcast
media), but mainly because it brings back memories of the days
when the
phrase "computer error" caught up with and overtook "dog ate my
homework".

((When was that, some time in the 60's?))

THOUSANDS OF US West customers recently got an unpleasant
surprise on
their telephone bills: an erroneous \$5 charge for switching to
new
long-distance carriers for certain in-state long-distance
calls. The
billing mistakes were due to a computer error.

Mike Schwartz, Phoenix Chapter ACM, PO Box 47302 Phoenix AZ 85068
(602) 436-4590 schwartz@acm.org Phoenix_Chapter@ACM.ORG
azmls@aztec.asu.edu

Reactivating Windows95 Screen Savers

Mich Kabay <75300.3232@CompuServe.COM>

06 May 96 09:13:55 EDT

As I reactivated the Windows screensaver this morning after
having turned it
off while ago, I suddenly realized that there is a problem with
the way
Windows95 handles the reactivation. Here is a scenario for what
can happen:

The user--

- 1) Sets a password in any Windows95 screen saver.
- 2) Disables the screen saver for a while.
- 3) Forgets Windows95 screen-saver password.
- 4) Forgets that there even was a password on your Windows95
screen saver.
- 5) Reactivates Windows95 screen saver.

The user has now reactivated the old, forgotten password and will be locked out (at least temporarily) of Windows95 files) as soon as the user selects the OK key.

Moral #1: Any software which allows a passworded function to be deactivated and then reactivated should require that the password be verified before allowing reactivation.

Moral #2: Before deactivating your Windows95 screen saver for an extended period, disable the password.

An alternative: to have much the same effect as disabling the Windows95 screen saver, set its delay period to a longer time that is unlikely to bother you during your normal work cycle (e.g., 15 minutes) rather than disabling it altogether.

M.E. Kabay, Ph.D. (Kirkland, QC) / Director of Education,
National Computer Security Association (Carlisle, PA) / <http://www.ncsa.com>

⚡ Re: AOL censors British town's name! (Miller, [RISKS-18.10](#))

Xcott Craver <caj@math.niu.edu>
Wed, 8 May 96 08:21:27 CDT

>> 1) Use PGP.

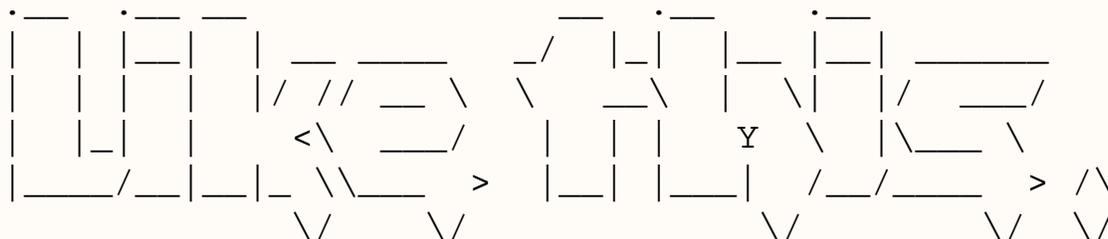
>

>This does not help. What if the output of PGP encryption innocently

>contains the byte sequence 0x63 0x75 0x6E 0x74? Being

gibberish, you didn't
>check - but the computer may, and censor it. There are similar
problems
>with uuencode, rot13, etc. Sigh!

There is a public domain computer program known as "figlet."
What it
does is turn text into large letters made of ASCII characters,



Normally, figlet is used only for aesthetic reasons, but
certainly one
sees its potential for bypassing "decency filters." Figlet
fonts range
from the huge to the relatively tiny, and it is quite easy to
see that a
figletized message will not contain any potentially indecent
random strings.
Yet more proof that brute regular-expression searching is an
ineffective
method of weeding out indecent speech.

Of course, aside from the obvious disadvantages of using big,
tacky
letters, there is the problem that enough people writing in
figlet will
alienate anyone whose online service software uses a
proportional font. I'm
not sure offhand if AOL's interface still does, but a couple
years ago
some people on the anti-aol group "alt.aol-sucks" actually
advocated piping
articles through figlet for just this reason!

Scott Craver -- Caj@niu.edu -- <http://www.math.niu.edu/~caj/>

⚡ Re: AOL censors British town's name! (Miller, [RISKS-18.10](#))

Dave Horsfall <dave@fgh.oz.au>

Thu, 9 May 1996 18:07:52 +1000 (EST)

In [RISKS-18.10](#), Peter Miller wrote: ``What if the output of PGP encryption innocently contains the byte sequence 0x63 0x75 0x6E 0x74?''

This actually happened to me! I always PGP-sign my messages on the local (amateur) packet radio network, to discourage forgeries, and many people run a "naughty word" filter to protect themselves. One day, my "signature" had the "f" word in it...

Dave Horsfall VK2KFU dave@fgh.oz.au Ph: +61 2 9957-4224 Fx: +61 2 9922-5286

FGH Decision Support Systems P/L, 77 Pacific Hwy, Nth. Sydney, 2060, Australia

[... as did the AUSTRIAN gerundive town name I mentioned in [RISKS-18.08](#),

which I misattributed as GERMAN. A correction is noted in the SRI archive copy of that issue. PGN]

⚡ Re: Odds of an accident for the Challenger

hal lewis <hlewis@physics.ucsb.edu>

Sat, 11 May 1996 08:38:44 -0800

I didn't want to get involved in the thread that involved NASA's pre-Challenger risk estimates, but it's probably better to set the record straight. (The reason for reluctance is that people who think of risk as a single probability are usually going to misuse the number they

find,
whatever it is. There is more to risk than a probability.
Especially when
that number has an uncertainty of more than a factor of ten.)

In the glory days of Apollo NASA had pretty good risk estimates available
(by the standards of those times), but tended to suppress them for reasons
like the one mentioned above. If you say that the risk of failure is one in
a hundred, give or take a factor of ten, your decision is likely to be
different for a chance in ten and for a chance in a thousand, so the people
who made the decisions found that the risk estimates didn't help them much.
And they didn't care about the social and scientific benefits of actually
knowing something. (That's a pattern throughout the risk business, that
people cling to bottom-line numbers as if they were gospel, either not
caring about uncertainties or not understanding them.)

Anyway, NASA lost interest in risk analysis, but there were still a few
competent people toiling away and making the estimates. By the time of
Challenger there were decent (within a factor of ten or so) estimates
available at NASA HQ, but the upper management treated them like the
Apocrypha. And the attitude spread (largely because of the beneficial
politics) that space travel was now "safe," leading to the mindset that
Feynman found in the engineers he talked to after the accident. They really
believed (in part because they didn't understand probability) that risks of
a chance in 100,000 were about right, despite all the evidence in the world

that that was a fantasy. (I also interviewed lots of NASA people after the accident, and found the same syndrome.)

Through it all, there were people at HQ who had pretty good analysis. There were also lots of little things (like the hydrazine fire potential) in which risk analysis revealed a hazard that top management talked its way around.

(Just a few months ago we found NASA management redefining the risk criteria just to avoid holding up a launch---that's the sort of thing that led directly to Challenger.) People who spoke about risk at HQ were treated as if they had leprosy (I tell you that from personal experience.) And out in the field, people took their cues from HQ. I personally asked Jim Fletcher (twice Administrator of NASA, including the period after the accident) to go public with risk estimates, and he always said he'd consider it. You can't sell that kind of promise for much in Washington.

Finally, after Jim had left NASA, he was asked at some public meeting what the risk of a disaster was, and he actually answered. He said a chance in seventy-two. There was indeed such a number available in an internal NASA report, but with the usual admonition of real experts that it's probably good to around a factor of ten. The author of that report, who is indeed a real expert, was horrified that the bottom line had been mentioned without the uncertainty. The same old reason---people will believe it to be TRUE, and bad decisions will be made.

So this is a case in which, as Alexander Pope would have said, a

little

knowledge is a dangerous thing. Some well-meaning people at NASA disliked

bottom lines because they were of little help in making the necessary

bottom-line decisions, while many of the engineers simply didn't understand

risk at all. Whenever anyone says that something is "safe" or "unsafe," they

don't understand risk. Through it all, decent analyses did exist, and were

available to, but ignored by, all the top management. It's still that way.

My judgment, not based on access to any recent analysis, is that the

probability of a disaster hasn't changed a great deal in recent years, but

that NASA management's complacency grows with each launch that is free of

disaster. Since the laws of probability never sleep, but people do, the

outcome is predictable. I once asked an astronaut (in connection with a

proposed change) whether he'd be willing to fly on top of that thing. His

answer (loosely quoted) was "Sure, because I'm an intrepid sort, but I

wouldn't want my best friends on the same flight." It's as wrong to let risk

paralyze you as it is to underestimate it. And it's a scam on the citizenry

to quote risk in terms of a single probability number. To say nothing of the

astronauts, who are a pretty good bunch. As Clint Eastwood would have said

if Dirty Harry had been an author, read my book.

Hal Lewis

✶ Re: Odds of an accident for the Challenger (Green, [RISKS-18.10](#))

Jordin T. Kare <jtk@s1.gov>

Wed, 8 May 96 13:25:48 PDT

>I have Volume I of the Report of the Presidential Commission on the Space

>Shuttle Challenger Accident (U.S. Gov't Printing Office, June 6th, 1986).

>Nowhere in this volume could I find a reference to the numerical odds

>of a shuttle accident.

In Volume II of "Technical Report on Preliminary Risk Assessment for Nuclear

Waste Disposal in Space", (E.E.Rice, NASA CR 162029, 2/28/82) there is a

discussion of Shuttle failure probability from early in the Shuttle flight

era. On P. 57, under "Standard (SRB) Space Shuttle":

"NASA does not publish or have in its possession 'official' reliability or

failure rate data for the space shuttle.... Plans are to continuously

upgrade problem areas as they are encountered on flights. The failure rates

for the Shuttle are actually corollaries to ALARA (As Low As Reasonably

Achievable, as in nuclear radiation risk)"

So there was no "official" reliability estimate. But the very next

paragraph says:

"Because of a NASA need to evaluate whether or not a destruct system on the

Shuttle during the early portion of the flight is worthwhile, NASA

contracted with Wiggins Company, Redondo Beach, CA, to perform a study

involving the hazards to the public of a failing Shuttle (Baeker, 1981). Another Wiggins study (Hudson, 1979) has also been conducted for the later portions of the flight profile to evaluate hazards when flying nuclear payloads (e.g., Galileo). The failure rates developed in these studies were based upon data developed for hardware in WASH-1400 (US NRC, 1975) and upon NASA committee reliability estimates for the SRB. The analysis was accomplished for only single-point failure modes, as have been identified in [various NASA and Rockwell references]. The Wiggins data also includes changes/modifications to failure rates resulting from an in-depth review by NASA Space Shuttle engineers...."

There's a summary table of results from the Wiggins study, which I won't reproduce in full, but a few of the entries are:

Failure mode	Failure rates	
	mean	lower
upper		
1. Tipover on pad	3.3E-5	1.6E-5
6.0E-5		
2. Loss of control and Tumble	2.0E-3 to 2.0E-4	
...		
5. Corkscrew motion from SRB TVC failure	4.2E-7	2.3E-7
7.4E-7		
6. Ext. Tank Punctured Liftoff to Staging	2.0E-7	8.4E-8
4.6E-7		
...and so on		

The dominant failure mode is Loss of Control and Tumble, at 1-in-500, which has a footnote: "Engineering Judgement from NASA for man-rated solid

propellant boosters."

Interestingly, there's a second set of data for a modified Shuttle with liquid-fuel boosters, for which the highest failure probability is Liquid Booster Recontact at Separation, $1.3E-5$. So a Shuttle with liquid boosters was estimated to be about 15 to 150 times safer than one with solids.

The appendix to this report has much more detailed breakdown of the risk analysis, for the Shuttle itself and for other potential failure modes for nuclear waste disposal.

[References were:

Baeker, J.B., 1981, Space Shuttle Range Safety Hazards Analysis, Tech. Report 81-1329, J.H. Wiggins Co., Redondo Beach, CA.

Hudson, J.M., 1979, Development of STS Failure Probabilities, MECO to Payload Separation, Tech Rpt 79-1395, J.H. Wiggins Co.....]

Jordin Kare

Internet in danger

<gep2@computek.net>

Fri, 10 May 1996 15:14:15 -0700

(via frantz@netcom.com (Bill Frantz) and minow@apple.com (Martin Minow))

The following was distributed to Cypherpunks. I have not verified it (or summarized it). The translation appears accurate, however.

Martin Minow

minow@apple.com

----- Attachment follows -----

You think we're having problems here in the USA with the idiotic CDA, right?

I just received the following message from a colleague and friend who

operates a large ISP in Paris, France. The translation is mine, and I can't

assure its total accuracy, (anyone who sees an error on my part, please

correct it for me). I'm leaving the original French so that the original

intent of the message can be viewed. [Bill Frantz]

<----- Begin Forwarded Message ----->

Return-Path: opinions@storm.certix.fr

Date: Thu, 9 May 1996 19:42:12 +0200

>From: Communication client <opinions@storm.certix.fr>

To: gep2@storm.certix.fr

Subject: Internet en danger

> Cher(e)s abonne(e)s,

Dear Subscribers,

> Nous n'avons malheureusement plus la possibilite de vous laisser acceder

au service de News. Exception faite des news world-net.

communnaute,

world-net.support, fr.network.internet.

Unfortunately, we no longer have the possibility to let you access Usenet.

The only exceptions are the newsgroups "world-net.communnaute", "world-net.support", and "fr.network.internet".

> En effet, la justice francaise rend actuellement World-Net responsable

de tout ce qui est diffuse sur Internet ; j'ai ete

personnellement, en tant

que responsable de World-Net, mis en examen hier parce que des images a

caractere pedophile, venant de l'autre bout du monde etaient accessibles par notre service de News. Aujourd'hui les news, demain peut-etre le web.

The French courts currently hold World-Net responsible for everything which is distributed on the Internet; I was personally, as director of World-Net, interrogated yesterday because some pedophile images, coming from the other end of the world, were accessible through our News server. Today Usenet, tomorrow perhaps the Web.

> La majorite d'entre vous connait le fonctionnement du reseau Internet et sait bien que World-Net n'est que votre transporteur sur ce reseau. Cependant nous n'avons pas le choix.

The majority of you understand the functioning of the Internet network and clearly realize that World-Net provides merely your access to this network. It's not a matter of our choice.

> Nous diffuserons sur notre serveur Web l'ensemble des informations citees dans la presse et a la television concernant ce dossier.

We will distribute via our Web server complete information as cited in the press and on television concerning this whole affair.

> Si vous voulez soutenir World-NET, envoye un mail de soutien a opinions@worldnet.net.

If you want to support World-NET, send a mail message of support to "opinions@worldnet.net".

> Sebastien Socchard

Directeur de World-Net.

(director of World-Net)

>Ci-joint le communique de presse de l'A.F.P.I., que nous
remercions pour
leur soutien :

Here is the press release from the A.F.P.I., which we thank for
their
support:

>COMMUNIQUE DE PRESSE DE L'A.F.P.I.

Association Fran=Claise des Professionnels d'Internet

PRESS RELEASE FROM THE A.F.P.I.

French Association of Internet Professionals

> Mardi 7 Mai 1996

Tuesday, May 7, 1996

> Affaire: Newsgroups/Pedophilie/Internet: deux dirigeants en
gardes a vue.

Affair: Newsgroups/Pedophilia/Internet: Two directors
<translation?>

> Resume: "Nous demandons a l'ensemble des providers fran=Clais
et des
administrateurs des reseaux d'universites de fermer l'accès a
tous les
Newsgroups, afin que plus un seul Newsgroup ne soit accessible
du territoire
fran=Clais, du moins tant que les fournisseurs d'accès n'auront
pas en
France un statut clair".

Summary: "We ask all French ISPs and administrators of
University networks
to close access to all Usenet newsgroups, such that no longer
will even one
single Newsgroup will be accessible from French territory, at
least until

French ISPs have a clear legal position within France."

> Depuis 48h00 les deux dirigeants des sociétés FranceNet et WorldNet sont en garde a vue pour avoir simplement fait leur metier consistant a fournir l'acces a l'Internet...

Since about 48 hours, two directors of French companies, "FranceNet" and "WorldNet" are <translation?> for having simply done their job, consisting of providing access to the Internet...

> En effet, la Section de Recherches de Paris de la gendarmerie Nationale a procede lundi a leurs arrestations et a la saisie de leurs materiels, pour avoir diffuse au travers des Newsgroups des images pedophiles. Ces Newsgroups et les images qu'ils abritent, sont tous produits a l'etranger et rapatriees comme le font la plupart des fournisseurs d'acces fran=Clais via les serveurs de News de Transpac, filiale de France Telecom.

The Research Section in Paris of the National Gendarmes started on Monday their arrests and seizures of equipment, for having distributed pedophile images through the Usenet newsgroups. These Newsgroups and the images they contained (?) are all originated abroad and brought into France as is done by the majority of French access providers via the News servers of Transpac, which is a subsidiary of France Telecom.

> Alors que la justice, dans une affaire similaire mais liee cette fois a des contenus racistes ou revisionnistes presents sur l'internet, ne s'est pas encore prononcees a l'encontre de neuf fournisseurs d'acces,

alors que le
ministere des Postes et des Telecommunication, au travers de son
ministre
Fran=Clois Fillon assurait encore recemment qu'en aucun cas les
fournisseurs
d'accès ne pouvaient =CDtre tenus pour responsables des contenus
qu'ils ne
produisaient pas et qui circulaient sur l'internet, alors que le
lieutenant-colonel Browne, commandant la SR de Paris, reconnait
lui meme que
les serveurs en question recevaient, stockaient et distribuaient
(tout comme
Transpac) mais ne produisaient pas ces Newsgroups, deux hommes,
deux chefs
d'entreprises sont aujourd'hui en prison simplement parce que
les autorites
n'ont toujours rien compris a l'Internet et a son fonctionnement.

The [French] courts, in a similar case but this time based on
racist or
revisionist contents present on the Internet, have not yet
passed their
judgement regarding nine ISPs, although the Ministry of Post and
Telecommunications, through its minister Francois Fillon, stated
again
recently that in no case can access providers be held
responsible for
content that they do not produce and which circulates via the
Internet, and
although Lieutenant-Colonel Browne, commander of the Research
Section in
Pairs, admitted himself that the servers in question receive,
store, and
distribute (the same as Transpac), but do not produce these
Newsgroups, two
men, two company directors, are today in prison simply because
the
authorities still haven't understood anything about the Internet
and its
functioning.

>La plupart des providers rapatrient de 6 a 8 000 Newsgroups
chaque jour,

soit plusieurs centaines de milliers de messages, pouvant également contenir des images. Parmi ces messages ils y a incontestablement des contenus contraire a la loi fran=Claise (sans doute moins de 5%), tout comme il peut en circuler par la poste, ou dans les soutes a bagage d'Air France. Il est materiellement impossible pour un provider de controler l'ensemble du contenu des messages des Newsgroups, il lui est eventuellement possible de supprimer l'accès a ceux dont le titre est de fa=Clon evidente contraire a la loi (ex.alt.binaries.pedophilia...), ce qui n'empêchera pas le lendemain de voir surgir un nouvel intitule pour remplacer le Newsgroup censure.

Depuis plusieurs mois deja les membres de l'AFPI (Association des Professionnels de l'Internet) dont FranceNet est l'un des fondateurs, ont spontanement decide de supprimer l'accès a une vingtaine de Newsgroups dont le simple libelle ne laissait aucun doute quant au caractere illegal de leurs contenus.

The majority of providers import from six to eight thousand Newsgroups each day, therefore several hundred thousand messages, any of which could also contain images. Among these messages there are incontestably some contents which are contrary to French law (no doubt less than 5%), just as they could circulate through the mails, or in the baggage holds of Air France. It is materially impossible for a provider to check the contents of all Newsgroup messages; it is possible to block access to those whose title is clearly contrary to the law (e.g. alt.binaries.pedophilia...), which wouldn't

prevent the following day to see a new group appear to replace the censored one. Since several months already, the members of the AFPI (Association of Internet Professionals), of which FranceNet is one of the founders, have spontaneously decided to suppress the access of about twenty Newsgroups whose title left no doubt as to the illegal character of their contents.

> Aujourd'hui ce sont les Newsgroups qui sont visés, demain ce sera sans doute le tour du Web. Si les fournisseurs d'accès, qui nous ne le répéterons jamais assez, ne sont que de simples transporteurs facilitant l'accès à un réseau, peuvent être emprisonnés, avec comme simple pièce à conviction un contenu produit au Canada ou en Australie, nous allons assister purement et simplement à la mort de l'internet en France.

Today it is the Newsgroups which are wiped out, tomorrow it will be doubtless the Web's turn. If access providers, which we can never emphasize enough, are but the simple transporters facilitating access to a network, can be imprisoned, due to the singular cause of an item produced in Canada or in Australia, we are going to see, purely and simply, the death of the Internet in France.

>En signe d'indignation, de protestation et de solidarité envers nos confrères FranceNet et Worldnet, le fournisseur d'accès ImagiNet, également membre fondateur de l'AFPI, a décidé de fermer purement et simplement l'accès à tous les Newsgroups. Nous demandons à l'ensemble des

providers fran=Clais et des administrateurs des reseaux
d'universites d'en
faire autant afin que plus un seul Newsgroup ne soit accessible
du
territoire fran=Clais, du moins tant que les fournisseurs
d'acces n'auront
pas en France un statut clair.

As a symbol of indignation, of protest, and of solidarity with
our brothers at
=46ranceNet and WorldNet, the access provider ImagiNet, also a
founding
member of the AFPI, has decided to purely and simply close
access to all
newsgroups. We ask all French ISPs and administrators of
University
networks to do the same, such that no longer will as much as a
single
Newsgroup will be accessible from =46rench territory, at least
until access
providers in France have a clear legal status.

>Nous esperons sincerement que cet appel sera suivit par
l'ensemble des
prestataires de connexion internet.

We sincerely hope that this call will be followed by all
Internet access
providers.

>Nous nous excusons aupres de nos abonnees pour la gene ainsi
occasionnee par
une telle decision, mais nous savons que vous la comprendrez et
que la
majorite d'entre vous nous soutiendrons dans cette action.

We ask the understanding of our subscribers for the
inconvenience caused by
such a decision, but we know that you will understand and that
the majority
of you support us in this action.

> Patrick Robin

President d'ImagiNet.
robin@imaginet.fr
Tel 43 38 10 24

<----- End Forwarded Message ----->

Please feel free to forward this message to all appropriate venues. "If we don't all hang together, we shall assuredly all hang separately." ---Thomas Jefferson (?)

Gordon Peterson <http://www.computek.net/public/gep2/>



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 18: Issue 12

Wednesday 15 May 1996

Contents

- [Software piracy](#)
[PGN](#)
- ["Call Girls" web site \[Name withheld by request\]](#)
- [Morphing Character 217 in Macintosh Geneva Font](#)
[Paul Robinson](#)
- [The risk of adding protection](#)
[Ray Todd Stevens](#)
- [Troubleshooting ValuJet after the crash](#)
[Phillip C. Reed](#)
- [Re: Internet in danger](#)
[Jim Carroll](#)
[Kevin Stock](#)
- [Re: Odds of an accident for the Challenger](#)
[Michael Wild](#)
[John W. Cobb](#)
- [Discussion Drafts of Medical Records Privacy Legislation](#)
[James Love](#)
- [The SEI Software Engineering Symposium](#)
[Carol Biesecker](#)
- [Info on RISKS \(comp.risks\)](#)

✶ Software piracy

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

Tue, 14 May 96 8:43:35 PDT

"Software Pirates Loot Silicon Valley;
Hong Kong street vendors hawk hot software"

An article by Jeff Peline in the **San Francisco Chronicle**, 14 May 1996, p. C1 aptly summarizes some of the basic problems of software piracy:

* Two CD-ROMs with more than 100 programs (Windows 95, Windows NT, AutoCad, LotusNotes, Xing's Mpeg, ...) valued at \$50,000 go for \$70 from a Hong Kong street vendor (pushing something that looked like a hot-dog cart). These items (and many conventional CDs as well) come from pirate operations in southern China [apparently turning out legitimate products when the "inspectors" are around for an hour or so, and hot stuff the rest of the time -- on a 24-hour production schedule].

* Pirated software costs an estimated \$12 billion annually worldwide.

* "More than half of all software in existence today is lost to piracy."

* An estimated 98% of the software sold in China is pirated -- to the tune of 200 million copies a year; in Brazil it is 95%, in Russia 94%.

Korea is at 78%, Japan at 67%, the U.S. at 35%, according to a chart

attributed to Glenco Engineering, Inc.

[No one seems to mention the devious opportunity for Trojan horses being added inside the pirate shrinkwrap.]

[If it's a floppy, it might be a copy.
If it's a disk, you're also at risk.
If it's a pirate, the vendors are irate.
To avoid such frustration,
try: Free Software Foundation.
(Not enough BurmaShavian literature anymore?)]

[Considering the volume and issue, this item must be an 18.12 OVERTURE. PGN]

⚡ "Call Girls" web site

<[Name withheld by request]>
Mon, 13 May 1996 15:09:47 -0700 (PDT)

Just fire up Ye Olde Web Browser, and open the URL
[URL withheld by Moderator's
Standards. PGN].

It'll show you a curvacious, scantily-clad female member of our species, ask you for your phone number (including area code), and then a female with a sexy voice will call you right back and say, um, "things" (ahem), to you. Yes, that's right, a call-back phone-sex system on the Web.

But of course, it doesn't take much imagination to realize you don't have to type in **your** phone number. How about your boss's? Or his wife? Or your not-so-favourite right-wing member of parliament/congress? This could be one of the best ways to get 'net censorship going: have these sexy voices call up a random, powerful right-wing politician. This is just

a variation
of the old "order a large pizza with all the toppings to the
house across
the street" trick we loved to do as teenagers. Except the risks
are
potentially more dangerous.

⚡ Morphing Character 217 in Macintosh Geneva Font

Paul Robinson <paul@TDR.COM>

Mon, 13 May 1996 08:09:13 EDT

I discovered an unexpected condition when attempting to do some
printing of
a document created on the Macintosh, in that the character code
using ASCII
217 in the Geneva font does not appear onscreen the same way
depending on
what size it is.

I suspect this is an issue with other characters and character
sets. I know
there is a feature to select a certain character, usually a
"box" to display
in place of characters not defined for a certain font, in order
to show that
something is there, not merely either a blank or nothing at
all. Since I
would expect that to be consistent, that is acceptable, and in
fact, much
more desirable behavior, e.g. if the character is undefined in a
particular
character set, a square is printed, to show that the character is
unprintable (undefined) in that set.

But **this** behavior is both unexpected and undesirable.

What I discovered is that a character in a specific font on the
Macintosh

can be "amorphic", in that it can be a different appearance depending on whether it is printed or displayed on screen, and depending on what size it is displayed at. Now, I'm not talking about the difference between the appearance of, for example, the letter "S" when shown onscreen and when printed with a 9-pin dot-matrix printer and the appearance when printed with a 300dpi laser or inkjet. No, I'm talking about selecting, say, an character containing the image of a Star of David, and printing out a Hammer and Sickle!

Some characters on some sets produce some interesting effects, including such symbols as the entire Zodiac; various stars, both circled and squared, white and black; arrows going in 8 directions, various other symbols such as icons of telephones, scissors, greek and mathematical symbols, and many others.

These symbols can be useful for various enhancements to a document. For example, one could print a coupon, and use the scissor symbol on the dotted line with the words "Cut Here" to make a much nicer looking image.

But when displaying some sets, what you see isn't always what you get!

Here is an exact explanation of what I did and what I discovered:

I created a macro using the Word Basic programming language that is included as a part of Microsoft Word for the Macintosh. This macro created every character in the Ascii set from 0 to 255. I deleted all the

nonprinting characters (0-31), and left the rest that did show.

I changed the default font, which happens to be Times, to various fonts in the collection we have for the purpose of creating a display of all the different symbols and special effects characters such as arrows, borders, and indicators such as superscript and subscript characters.

In one case, When I changed the font Geneva from 12 to 20 point, I noticed something odd. The character I later determined to be ASCII 217, in Geneva 12 point, appeared as an image of a rabbit. In 20 point, however, that character metamorphized into the image of a Macintosh computer!

It gets more interesting. I tried the different font sizes available, and this is what I saw:

Point	Character
8	Upper Case Y with two dots above
9	Image of a sheep
10	Image of a Macintosh
11	Upper Case Y with two dots above
12	Image of a rabbit
14	Image of a dog
16	Upper Case Y with two dots above
18	Image of a sheep
20	Image of a Macintosh
22	Upper Case Y with two dots above
24	Image of a rabbit
26,28,36,48,72	Upper Case Y with two dots above

The behavior appears to be consistent; the "special" images reappear at the doubling of the character (except the "dog"). What is notable about this is that when the character set is printed out on an Apple color inkjet printer,

what does appear - at the appropriate 8 to 72 point size as is used - is the specific character, the upper case Y with two dots above. (I can't yet remember the exact name for that mark, I think it is called an umlaut.)

As for the risks, the example I gave above is pretty clear. (Oh yes, the Star of David and the Hammer and Sickle are available, but fortunately they are different characters in different fonts!)

I am reporting this because I believe that if it happens in one font it can happen in others. Consider a font designed so that the \$ appears as the British pound sterling when printed, or the #, and it could cause misunderstandings, perhaps even legal problems. Especially if - and it is possible - the printed output, having been checked several times in previous revisions, is merely given a cursory glance when reprinted using a slightly larger font.

It is well understood that Postscript is a programming language, and with all the risks and benefits that implies. But font files may or may not be, depending on the system or the application, and that opens up a whole new can of worms.

Unexpected behavior in a rarely-used symbol is, in-and-of-itself not a big deal. But in other contexts it could be, and thus I considered the issue to be worth reporting.

Paul Robinson, General Manager, Tansin A. Darcos & Company/TDR, Inc.

[I am curious about the upper-case Y-umlaut. German, Turkish, and Swedish

(for example) use umlauts (as does English, for diaeresis), but I have

never seen an upper-case Y-umlaut. I have seen Dutch names (Edsger

Dijkstra's, for example) in handwritten Dutch appear with the i and j run

together as if they formed a "y", with the dots over the i and j appearing

as a y-umlaut (in lower case only). Perhaps this is one of the Power(book) Morphin' Dangers? PGN]

⚡ The risk of adding protection

"Ray Todd Stevens" <raytodd@tima.com>

Wed, 15 May 1996 13:13:01 +0000

I ran into an interesting risk recently. A computer is located where it is

hard to gain physical access. This computer some times needs reseting. To

this end a system to remotely turn the power off and back on was installed.

Recently it was decided that this computer must operate in the case of a

power failure. As a result a UPS was installed. You guessed it, we now

can't remotely reset the computer.

Ray Todd Stevens Senior Consultant Stevens Services R.R. # 14
Box 685

Bedford, IN 47421 (812) 279-9394 Raytodd@tima.com

⚡ Troubleshooting ValuJet after the crash

"Phillip C. Reed" <reedpc@libbey.com>

Wed, 15 May 1996 09:46:44 -0400

As part of the aftermath of the ValuJet Florida crash, the FAA announced that they will be scrutinizing all of ValuJet's procedures, including flying inspectors in the cockpit to watch the crew at work. Exactly what they expect to find doing this is cloudy to me, given the 'observer effect'. It's axiomatic that the crew will behave differently with an inspector peering over their shoulder.

The RISK is that the FAA will waste a lot of time and energy looking at something that won't give them useful information. Perhaps it's time for video cameras in the cockpit?

Phil Reed Libbey Inc reedpc@libbey.com

🚨 Re: Internet in danger ([RISKS-18.11](#))

"Jim Carroll" <PJCARROL@ca.oracle.com>

Tue, 14 May 1996 11:04:05 -0400

I seem to recall hearing a CBC Radio report on a similar situation developing in Germany in, if memory serves, January of this year. The target which they were attempting to quash was hate literature. Surprisingly (because I'm Canadian), the report mentioned that most of the hate literature on the Internet originates in Canada. (This begs the question of the source and reliability of this statistic.)

As I remember it, the German government was taking issue with this material, and figured (similar to the case in France) that the best approach was to hold the ISPs legally accountable. The reaction on the part of the ISPs was to cut off any newsgroup deemed to be inappropriate.

What surprises me is that nobody is fingering the telcos using the same slippery-slope arguments, ie, providing the hardware and the bandwidth.

Perhaps someone with a better recollection of events than I could give this story better clarity.

Jim Carroll <pjcarrol@ca.oracle.com> Principal Consultant, Core Consulting
Oracle Corporation Canada Inc.

🔥 Re: Internet in Danger ([RISKS-18.11](#))

Kevin Stock <kstock@Auspex.Com>
Wed, 15 May 96 04:14:17 PDT

There have been similar reports to this from various places for some time. However, one extra detail did catch my interest; France Telecom (the French state-owned telephone service) recently launched its own Internet access service under the name 'Wanadoo'. I wonder if it will also withdraw from providing the News.

✶ Re: Odds of an accident for the Challenger (Green, [RISKS-18.10](#))

Michael Wild <mwild@iee.org>

Mon, 13 May 1996 23:44:17 -0700 (PDT)

A discussion of the Rogers report from the perspective of organizational psychology can be found in Chris Argyris, *Overcoming Organizational Defences* (Allyn & Bacon, 1990). Inter alia, he says "... the Rogers Commission unwittingly strengthened the organizational routines that caused the problems in the first place." I would commend Argyris' book to anyone seeking to understand the attitudes that underly many of the RISKS discussed in this forum.

Michael Wild <mwild@iee.org>, <michael@kyrie.demon.co.uk>

✶ Re: Odds of an accident for the Challenger (Green, [RISKS-18.10](#))

John W. Cobb <cobbjw@ornl.gov>

Wed, 8 May 1996 18:22:05 -0400

>Nowhere in this volume could I find a reference to the numerical odds
>of a shuttle accident.

A lot of what Feynman's personal conclusions are not in the volumes.

Perhaps you remember the minor flap about Feynman's addition of a separate appendix.

However, Feynman did publish several other accounts (and some video interviews) discussing these issues, including the probability of failure.

I don't remember the exact reference source but some places to look are:

1) Feynman's "So what do you care what other people think?" (or some similar title).

2) A Cover story article in Physics Today soon after the report was issued.

Both of these are good reads in and of themselves as well as being excellent supplementary sources on the Challenger episode.

Feynman's role on the Roger's commission raises another issue that is worthy of discussion here. Do we help or exacerbate risks with our methods of ex-post facto accident investigations (Challenger, air-crashes, Exxon Valdez, ...) ?

Feynman seemed to feel that some very important issues about the management structure at NASA were not included in the Roger's report and that consequently were not being addressed. This does not include items in the report that have not been vigorously pursued (a debatable proposition in and of itself).

Do investigations reveal problems and fix them or do they simply serve to identify scapegoats? What's more, how do we define investigation ground rules to favor the former over the latter?

These are the critical questions to ask in order to reduce the

probability
of another challenger

John W. Cobb, Off. Computing&Network Management, Oak Ridge
National Laboratory
MS-6486 Oak Ridge, TN 37831-6486 1-423.576.5439 cobbjw@ornl.gov

✦ Discussion Drafts of Medical Records Privacy Legislation

James Love <love@tap.org>
Tue, 14 May 1996 19:05:23 -0400 (EDT)

[Sent to RISKS via Stanton McCandlish <mech@eff.org>. RISKS generally eschews such postings. However, this one may have broad appeal to readers in the U.S., and far-reaching implications. PGN]

Re: Getting Copies of "Discussion Drafts" of Med Privacy Bill Online

This is a sign-on letter to Senators Kassebaum and Warner, asking that the Senate make copies of its "discussion drafts" of S. 1360, the Medical Records Confidentiality Act, on the Internet. The discussion drafts reflect the current versions of the controversial legislation, after negotiations between various Senators and lobbyists.

Currently these drafts are only distributed in paper, and are mostly available to Washington DC lobbyists. Senator Kassebaum controls access to the discussion drafts, and Senator Warner is in charge of Senate rules on topics such as public access to Senate documents.

The letter has been signed by Gary Ruskin, Director of the

Congressional

Accountability Project, Lori Fena, Director of the Electronic Frontier

Foundation, James Love, Director of Consumer Project on Technology, and Jim

Warren, a well known computer journalist and information activist. To add

your name, send a note to Gary Ruskin at gary@essential.org.

The letter follows:

Senator Nancy Kassebaum, Chair
Committee on Labor and Human Resources
428 Dirksen Senate Office Bldg
Washington, DC 20510-6300

Senator John Warner, Chair
Committee on Rules and Administration
305 Russell Senate Office Bldg
Washington, DC 20510-6325

Dear Senators Kassebaum and Warner:

We are writing to express the frustrations of many American citizens who cannot effectively monitor the actions of the U.S. Congress, because the Senate does not give ordinary citizens the same access to key legislative documents that it gives to interest groups that can afford full time lobbyists. Our immediate concern is the refusal of the Senate Labor Committee to provide online access to a series of discussion drafts of S. 1360, the Medical Records Confidentiality Act. This controversial legislation seeks to pre-empt state laws in favor of a federal system regulating access to personal medical records. The legislation is controversial and complex and the stake holders are many. Privacy and

consumer groups say the legislation provides too much access and too little privacy, while industry groups are pressing for even easier access to identified medical records.

The legislation was introduced last October. Beginning in April, the Committee on Labor and Human Resources has prepared several "discussion drafts" for a new chairman's mark. These drafts have been given to lobbyists, but the Committee staff has refused to make the text of the drafts available on the Internet where they would be readily available to the general public. As a consequence, as Equifax, IBM, Dun & Bradstreet, TRW, Blue Cross, Aetna, and other groups with full-time lobbyists read each and every new discussion draft, the general public mistakenly believes the October 24, 1995 version of the bill represents the relevant text of the legislation.

Why keep the discussion drafts from the general public? The bill is very long, and it is costly and difficult to distribute the bill in the paper formats. Most citizens don't have any way of even knowing that the various discussion drafts even exist.

With efforts to push for a rapid mark-up on S. 1360 it seems urgent to resolve this issue soon. More generally, however, the Senate should adopt new rules about access to the various types of "unofficial" drafts of bills, including committee prints, managers amendments, chairman's marks, and widely disseminated discussion drafts, which are the real stuff

of the legislative process. The text of these important documents should be placed on the Internet for the benefit of the general public, as soon as they are made available to Washington lobbyists.

Sincerely,

Gray Ruskin, Director, Congressional Accountability Project
(Member, Advisory Committee, Congressional Internet Caucus)
gary@essential.org

Lori Fena, Director, Electronic Frontier Foundation, lori@eff.org

James Love, Director, Consumer Project on Technology, love@tap.org

Jim Warren, tech-policy columnist and open-government advocate
Government Technology Magazine, MicroTimes Magazine, etc.
345 Swett Rd., Woodside CA 94062; voice/415-851-7075
jwarren@well.com

To add your name to this letter, send a note to Gary Ruskin.
His contact info is:

Gary Ruskin gary@essential.org 202/296-2787; fax: 202/833-2406

James Love, Center for Study of Responsive Law, P.O. Box 19367,
Washington DC
20036 202/387-8030 Consumer Project on Technology; love@tap.org
with webpages.

The SEI Software Engineering Symposium

Carol Biesecker <cb@SEI.CMU.EDU>

15 May 1996 14:59:12 GMT

[Starkly abridged by PGN]

The SEI Software Engineering Symposium
Achieving Maturity Through Technology Adoption
September 9 - 12, 1996
David L. Lawrence Convention Center
Pittsburgh, Pennsylvania

The SEI Software Engineering Symposium is an annual event hosted by the SEI to provide an opportunity for people to learn about practical solutions to software-related problems and the role of the SEI in assisting the development and adoption of those solutions. The primary goal of the symposium is to provide a forum to facilitate communication among the various sectors of the software engineering community and to help participants build collaborative relationships based on their shared interests.

The format of the symposium will include plenary sessions, tutorials, panel discussions, presentations, and birds-of-a-feather sessions on topics that fall within three broad topic areas that promise significant sustained impacts on the state of the practice in the coming decade.

Topic 1: Trustworthy Systems: Security, Reliability, Safety

As computer-intensive systems grow in scope, and as their information bases grow ever richer, the users have corresponding concerns and increased needs for confidence in these systems. Continued successful use of such systems requires a high degree of reliability and security from harmful intrusions. Presentations in this topic area will address aspects of systems that lead

them to be considered trustworthy or not. Such presentations will include descriptions of systems specifically called "trustworthy systems," but will also includes such related topics as system vulnerability, system reliability, and information warfare.

Topic 2: Engineering of Software-Intensive Systems

In recent years, primary concepts of program design and program construction have been influenced and even overturned by developments in such domains as software reuse, by research in such topics as software architectures, and by methodologies such as object-oriented construction. As these developments mature and become ubiquitous, an emerging common thread is the notion of composition of systems; this notion underlies technologies such as architecture design languages as well as new system-oriented approaches such as open systems. Presentations in this topic area will describe a number of these developments, such as recent work in patterned architectures, integration of heterogeneous commercial tools, and program understanding.

Topic 3: New Dimensions in Process and Risk

The Capability Maturity Model(SM) (CMMSM) has become the most widely used basis for achieving process improvement in software engineering, and it has provided a framework for the development of a number of other maturity models for improvement efforts within other domains. With the forthcoming release of the CMM Version 2.0, this vital aspect of software engineering enters a new phase. New developments, such as integration of measurement

technologies with the CMM, as well as extension of the model toward risk assessment, risk management, and Personal Software Process (PSP), are extending the domain of process improvement enormously. Presenters in this topic area will consider practical and theoretical issues related to the CMM (e.g., CMM integration), results of industrial-scale process improvement efforts, and issues surrounding process-related technologies (e.g., current capabilities in process enactment engines).

Plenary Sessions: Six keynote speakers representing the views of industry and government will provide different yet complementary perspectives on current concerns as well as issues forming just over the horizon. Invited speakers include representatives from government and industry.

A view from DARPA, where tomorrow's technology is being explored today, will highlight a number of important issues in software assurance. Speakers from the Department of Defense will address ways in which information is becoming increasingly important both as an asset and as a potential threat.

Industrial perspectives on the trials and successes in day-to-day practice will fill out the picture of the relationships among these various sectors as we approach the millennium, and how those relationships are changing with the times.

Who should attend?

To address the broad set of concerns represented by the software engineering

community, presentations will cover topics of interest to people with differing levels of knowledge and technical expertise. A range of topical sessions will be offered to discuss issues of concern to senior managers, senior technical staff, and practitioners. The structure of the technical program will focus on

1. fundamentals of a technology area for those new to the technology or those who need to brush up on key concepts and developments
2. state-of-the-art or state-of-the-practice discussions to outline the best industrial practices and the ways in which they improve the baseline on practices
3. experience reports detailing the results of using particular technologies or approaches to improvement
4. management issues and answers to some of the fundamental questions that determine if and when to adopt a technology, such as return on investment or other business-case analyses
5. transition plans for key technologies that are deemed "close to ready" for transition into routine use and that offer nontrivial, measurable improvements to adopters

Tutorials, Monday, September 9, 1996

- _____ Personal Software Process
- _____ Identifying Success Strategies for Software Process Automation
- _____ Planning the Cultural Dimensions of Improvement
- _____ Comprehensive Risk Management
- _____ How to Deploy Software Process Improvement
- _____ FODA for Pragmatists
- _____ Legacy System Reengineering
- _____ Goal-Driven Software Measurement

Plenary sessions, panel discussions, and presentations, are offered Tuesday, September 10 through Thursday, September 12.

CMM and Capability Maturity Model are service marks of Carnegie Mellon University. The SEI is a federally funded research and development center sponsored by the U.S. Department of Defense, and operated by CMU.

Contact Information

Events

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, Pennsylvania 15213-3890
FAX 412 / 268-7401

Internet: registration@sei.cmu.edu

[And look for their web page for details. Carol did not give

a URL, but many readers object to URLs as not meaningful in the fullness of time anyway -- and besides, preannouncements are of less interest in the long run. 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 18: Issue 13

Friday 17 May 1996

Contents

- [Netscape 2.02 RISK](#)
[Ed Felten](#)
[for Tom Cargill](#)
[Dirk Balfanz](#)
[Drew Dean](#)
[himself](#)
[and Dan Wallach](#)
- [Garfinkel/Spafford, Practical UNIX and Internet Security, 2nd ed.](#)
[PGN](#)
- [Static hypertext links to dynamic data](#)
[John Light](#)
- [Notebook theft](#)
[Denis Parslow](#)
- [Post-divorce wage gap statistic turns out to be computer error](#)
[Mike Coleman](#)
- [France ISP issues](#)
[Simson L. Garfinkel](#)
- [WWW "Bandwidth Exceeded" signals](#)
[Simon Higgs](#)
- [Re: Software piracy](#)
[Li Gong](#)

[\[-Alias\]](#)

[Simon Arthur](#)

● [Re: Troubleshooting ValuJet after the crash](#)

[James L. Coffey](#)

● [Re: Morphing Character 217 in Macintosh Geneva Font](#)

[Eric Fischer](#)

● [Re: "Call Girls" web site](#)

[Mike Rose](#)

● [Info on RISKS \(comp.risks\)](#)

⚡ Netscape 2.02 RISK

Ed Felten <felten@CS.Princeton.EDU>

Fri, 17 May 1996 17:11:34 -0400

SECURITY FLAW IN NETSCAPE 2.02

We have discovered an attack that allows a Java applet running under

Netscape Navigator 2.02 to generate and execute arbitrary machine code.

The attack combines a new security bug found by Tom Cargill with some ideas

previously discovered by the Princeton team. We have implemented a

demonstration applet that deletes a file. We are not yet releasing

technical details.

For more information, contact Ed Felten (felten@cs.princeton.edu, 609-258-5906), or see <http://www.cs.princeton.edu/sip/News.html>

Tom Cargill

Independent Consultant

<http://www.csn.net/~cargill/>

Dirk Balfanz, Drew Dean, Ed Felten, Dan Wallach

Dept. of Computer Science, Princeton University

<http://www.cs.princeton.edu/sip/>

✦ **Garfinkel/Spafford, Practical UNIX and Internet Security, 2nd ed.**

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

Fri, 17 May 96 10:19:12 PDT

Practical UNIX and Internet Security, Second Edition

By Simson Garfinkel and Eugene Spafford

O'Reilly & Associates, Inc., 1996

1004 pages. ISBN: 1-56592-148-8. \$39.95

This book is an extraordinarily successful effort to cram into a mere thousand pages (971+xxix+ORAads) almost everything you need to know about Unix and Internet security. It is a complete rewrite of the First Edition of 1991, and contains much new material. In terms of pages per dollar or cents per page, or much more important, the amount of money it can save you by keeping you away from a horrendous array of potential security problems, it is an incredible bargain. This is a keeper -- at least until the Third Edition comes out, perhaps in 2001. By then, the authors will be able to write much more definitively about Java and web browsers, which are treated only lightly in the Second Edition. (Too much happening, too fast?) Everything else, however, seems well covered and very nicely written. This is a very readable and very useful book, and deserves to be looked at by all of you.

[Note: Coincidentally, the first two errors I found in *PUIS2* relate to

RISKS: (1) on p.897, the host name for the RISKS archive site (which has been unix.sri.com since 1 Jan 1995) is listed as crvax (which lead me to discover that the old crvax **still** exists, and is what AltaVista picks up, but that it contains only issues through volume 16), and (2) on p.879, a typo! One of the great advantages of on-line books will be that errors will disappear as rapidly as they are found. For example, there are still a few copies of the first printing of my Computer-Related Risks book around with the crvax reference, whereas the third printing correctly has unix.sri.com! THIS PARAGRAPH IS FOR RISKS READERS. Please truncate if this minireview gets redistributed elsewhere. PGN]

✶ static hypertext links to dynamic data

John Light <John_Light@ccm.jf.intel.com>

Thu, 16 May 96 12:42:00 PDT

I was reading the home page of a subsidiary of a **very** high profile WWW player.

On it was the phrase "bringing [top rated] capabilities", where the bracketed words were a hypertext link. I followed the link to Stroud's Consumate Winsock Applications (<http://cws.wilmington.net>), directly into the appropriate category, where I found that the original product is **no longer top rated*!*. In fact it had disappeared from the list. I was

glad this happened because I had not seen Stroud's site before,
and the
updated list pointed me at several new products, which probably
are better
than the original.

The obvious risk is that pointing to any data **not** on your web
site
requires a commitment to a higher level of vigilance and on-
going support,
or you may be surprised by the consequences.

John Light

Notebook theft

"Denis Parslow (Almo Distributing)" <dgp@world.std.com>

Mon, 13 May 1996 08:57:35 +0000

PC Week's latest issue (I unfortunately don't have it to quote
from)
stated that last year 1 out of every 14 notebooks (sold?) was
stolen.

I wish I could quote the rest.

The risks would certainly include the importance of password
security, file
access, etc. if your data is **that** likely to be stolen/
compromised.

Denis Parslow, Engineering Mgr, Almo Distributing, Trademark
Computers

dgp@world.std.com <http://www.almo.com> <http://world.std.com/~dgp/>

✦ Post-divorce wage gap statistic turns out to be computer error

Mike Coleman <coleman@chez-gnu.cstp.umkc.edu>

Fri, 17 May 96 01:56 CDT

An AP wire story reports that sociologist Lenore J. Weitzman has stated that a widely publicized statistic in her study "The Divorce Revolution" was incorrect. (The statistic was that the standard of living for women's households dropped 73% in the first year following a divorce, while men's households rose 42%.)

According to the story, Weitzman "blames the loss of her original computer data file, a weighting error or a mistake in the computer calculations performed by a Stanford University research assistant."

Weitzman's data were examined by sociologist Richard R. Peterson, who determined that the correct figures were 27% and 10%, respectively.

Without knowing more about the dataset and how it was processed, one can only speculate as to exactly what sort of mistake was made. The magnitude of the error suggests, however, that in this case the error might have been discovered with a rudimentary cross-check, e.g., a histogram of the data or a manageable random subset.

(The article is currently available as 'http://www2.nando.net/newsroom/ntn/nation/051696/nation2_5387.html'.)

Mike Coleman, Ctr for Telecomputing Research, <http://ctr.cstp.umkc.edu/~coleman>

✶ France ISP issues

Simson L. Garfinkel <simsong@vineyard.net>

Thu, 16 May 1996 10:50:21 -0400

As a hobby, I run a small ISP on Martha's Vineyard. We have about 350 customers and have a Usenet feed. However, we specifically block the alt.binaries groups. The principle reason that we do this is to conserve our bandwidth: receiving alt.binaries would require that we triple our off-island throughput.

However, even if we did have the alt.binaries groups, I do not think that we would take a few particular groups. These groups are alt.binaries.pictureserotica.teen and alt.binaries.pictureserotica.children. From my point of view, these groups exist solely for the carriage of child pornography.

US law says that possession of child pornography is a crime. Usenet, unlike the web, places a copy of every message on your server's hard drive. Any organization that has these newsgroups within the United States (including AOL) is in violation of federal law.

I do not buy the argument that censoring the alt.binaries.pictureserotica.teen and alt.binaries.pictureserotica.children newsgroups will make a provider legally liable to any message that is sent over the Usenet because they are now exercising some sort of editorial control. There is a big

difference

between deleting individual messages for editorial purposes and the wholesale deletion of groups.

Simson Garfinkel, President, Vineyard.NET, Inc.

✶ WWW "Bandwidth Exceeded" signals

Simon Higgs <simon@higgs.com>

Thu, 16 May 1996 14:19:07 -0700

It finally happened. The web finally got it's busy signal. No, not the web server saying it's busy, since it's happily serving out other pages. User home-page bandwidth ran out. Is this a sign of metering to come? Or a result of refusing to meter user traffic?

Internet Direct have a policy of cutting off a user's web pages when they have exceeded a predetermined amount of web server bandwidth. This creates a substantial risk when renting web server space from an ISP for providing time sensitive, or critical support information.

I'm really disappointed at seeing this kind of interference from an ISP.

--- begin forwarded text

Date: Wed, 15 May 1996 22:31:05 -0700

To: simon@higgs.com

Subject: 4x4

X-URL: <http://www.indirect.com/www/a4x4/suzuki.html>

<http://www.indirect.com/www/a4x4/suzuki.html>

Bandwidth Exceeded

Unfortunately, due to the extreme load on our user web server, we have been forced to require each user to stay below a certain maximum daily bandwidth limit.

User a4x4 has currently exceeded his or her bandwidth limit of 26214400 bytes for the day. This bandwidth limit will be reset and the pages will become available again at 1600 MST.

If you are an Internet Direct customer with high web server bandwidth needs, you may want to investigate our GoSite Internet Server product.

We apologize for any inconvenience. We feel this new strategy will provide all of our users with increased speed and better overall performance on their web pages. If you have questions or concerns about this policy, please send e-mail to support@indirect.com.

--- end forwarded text

Simon Higgs e-mail: simon@higgs.com <http://www.higgs.com/>

✶ Re: Software piracy ([RISKS-18.12](#))

Li Gong <gong@csl.sri.com>

Thu, 16 May 1996 10:22:33 -0700 (PDT)

PGN in [RISKS-18.12](#) quoted San Francisco Chronicle's report that "Pirated software costs an estimated \$12 billion annually worldwide." I

do not support piracy and such, but would like to point out the grossly exaggerated nature of such reports. Use China as an example.

Suppose there is a total ban of illegal sales of pirated software. The net result is not that the US companies (or others) will immediately make a lot more money on these "sold" software. Instead, not many copies will be sold for the simple, economic reason. A case in point. The Microsoft Visual C++ I bought last year was US\$400+. This translates into about Chinese Yen Y3600, which is a decent gross annual salary of a university professor in China. Now how many copies of this software can you sell?

In the long run, a total ban may actually help the Chinese software industry to obtain a breathing space and to develop its own software standard/platform and all. This would be extremely bad news for companies such as Microsoft. A reasonable strategy (e.g., for the US software industry) would be to sell at heavily discounted prices that the local market can bear and wait for the purchasing power to grow.

Thus, instead of screaming the piracy nonsense, the US (and other countries) should see the reality and view the current situation as an extended battle to retain market share, with its typical associated cost in lost revenue.

Li Gong, SRI Computer Science Laboratory, www.csl.sri.com/~gong

✶ Re: Software piracy ([RISKS-18.12](#))

<[-Alias]>

Thu, 16 May 1996 12:46:11 -0700 (PDT)

I am amazed that this figure continues to be printed without anyone challenging it. This figure assumes that every person who pirates or purchases a pirate copy of program X would have instead bought the program. Obviously false.

> * Two CD-ROMs with more than 100 programs ... valued at \$50,000

The industry counts this as \$50,000 worth of losses. But in fact, I would be very surprised if anybody who purchased this disk installed both Win95 and WinNT, let alone AutoCad, Notes, or Xing's Mpeg.

-Alias

✉ **Re: Software piracy ([RISKS-18.12](#))**

Simon <chroma@mindspring.com>

Wed, 15 May 1996 00:31:47 EDT

Interesting. CD's cost about \$US3 each to manufacture, last I heard.

With such a markup, the people manufacturing the CD's must be making a fortune. No wonder they're so hard to stop.

> * Pirated software costs an estimated \$12 billion annually worldwide.

You could also look at it like this: Businesses save about \$12 billion annually through flexible adherence to software license

agreements.

> * "More than half of all software in existence today is lost to piracy."

Where'd it disappear to? :-)

> according to a chart attributed to Glenco Engineering, Inc.

Glenco Engineering, Inc. manufactures and sells copy protection devices.

See <http://www.glenco.com/> for details and the chart.

Not that I think their numbers are too high. In fact, it seems that in small

businesses in the US about 60% of all software is pirated. In large

corporations, compliance is probably well above 90%. For home users, I'd say

that maybe 90% has not been paid for. These are just my estimates from my

work as a consultant, having visited many businesses.

> [No one seems to mention the devious opportunity for

> Trojan horses being added inside the pirate shrinkwrap.]

Far be it from me to provide potential warning to software pirates, but

a person less honest and law-abiding than me might suggest that the greater

danger lies in being swindled by a hot-dog cart guy selling defective disks.

If you need it cheap / Don't buy from that creep.

If Hong Kong won't cut it / But it can't be legit

Think of how much money you'll save / When your software's from Burma (shave).

Simon Arthur chroma@mindspring.com

✶ Re: Troubleshooting ValuJet after the crash (Reed, [RISKS-18.12](#))

"James L. Coffey" <jcoffey@crl.com>
Wed, 15 May 1996 16:15:31 -0700

My experience (as an evaluator of nuclear power plant operators), is people tend to quickly forget that an observer is present, if the observer just watches and doesn't interrupt the operators as they carry out their tasks. Even if they try to do things in a different manner than they normally do, they also tend to lapse back into their normal operating mode after a while. In addition, it is generally pretty obvious to a trained observer when a crew is trying to "put on a show."

The RISK there is that they will make mistakes they normally wouldn't because they are not operating like they are used to and that causes communication and coordination problems and increases the chances of making an error.

: The RISK is that the FAA will waste a lot of time and energy looking at
: something that won't give them useful information. Perhaps
it's time for
: video cameras in the cockpit?

Video cameras, while a useful tool for review and debriefing, will often miss crucial actions. The RISK (or RULE) is that they always point to the wrong spot.

⚡ Re: Morphing Character 217 in Macintosh Geneva Font (Robinson, 18.12)

eric fischer <enf1@midway.uchicago.edu>

Wed, 15 May 1996 19:32:06 -0500 (CDT)

Paul Robinson reported the surprising behaviour of a Macintosh character which appears as Y-umlaut in most fonts but as symbols which vary with the font size in a few others.

The full range of these secret characters was documented in great detail in Volume I, Issue 2 of *_Macworld_* (May/June 1984), as a "treasure" that "only luck and wild fingers on the keyboard would have unearthed." The set of characters in current Macintosh fonts is larger than in the ones that were available in 1984 (so the special characters were not taking the spot reserved for Y-umlaut, but were in a location that would otherwise be empty, but happened to be typable with Option-Shift-Tilde) and, since all the fonts were bitmapped rather than scalable, and the only output device, the Imagewriter, matched the screen resolution exactly, there was no confusion caused by rescaling the fonts to match different output devices. So the risk of accidentally misusing these characters didn't come into being when they were placed into the fonts, but was instead when "legacy" fonts weren't updated to match newer notions of what Mac fonts should contain.

For the record, here are all the special symbols hidden in the original Mac fonts, not all of which are still shipped with current Macintosh software:

New York
hearts: 9, 18pt
robots: 12, 24pt
musical notes: 14pt

Toronto
boxes: 9, 18pt
vines: 12, 24pt
apples: 14pt

Chicago, London,
Monaco:
undefined

Geneva:
sheep: 9, 18pt
rabbits: 12, 24pt
birds: 14pt

all sizes:
Venice: chains
San Francisco: cars
Athens: footprints

Eric enfl@midway.uchicago.edu

⚡ Re: "Call Girls" web site ([RISKS-18.12](#))

Mike Rose <mrose@stsci.edu>

Thu, 16 May 96 12:29:27 EDT

The risk that call-back phone-sex will bring censorship to the net seems far-fetched. For starters, I'd bet a big bottle of crisco that those sexy voices won't be saying anything until they've got a credit card number.

Why would a politician receiving such a call, assuming he or she objects, blame the internet? The recipient doesn't know how the transaction to the call-back service was initiated and, even if they do know, does it really matter? Any legal restrictions should be placed on the actual service, not the ordering mechanism.

Mike

✶ Re: Internet in danger ([RISKS-18.11](#))

Mike Crawford <crawford@scipp.ucsc.edu>

Fri, 17 May 1996 12:26:41 -0700

There were two things that happened in Germany. In one case a local prosecutor got CompuServe to censor a couple hundred newsgroups.

In the other case, Web Communication's entire web server has been censored by Germany. I think they use packet filters to drop packets with www.webcom.com's IP address. This was done because a Canadian customer of Webcom's is a historical revisionist - his web page argues that the Holocaust never happened, and promotes Nazi politics, etc. Germany does not have complete freedom of speech - promoting Nazism is illegal there.

Germany's effort largely backfired because a number of other sites immediately provided mirrors for the Nazi. Webcom's other customers, mostly ordinary businesses, are blocked out from the whole nation of Germany.

Mike Crawford crawford@scruznet.com <http://www.scruznet.com/~crawford>

[This is an old story, but has not run in RISKS before. PGN]

✶ Re: Internet in danger

"Jim Carroll" <PJCARROL@ca.oracle.com>

Thu, 16 May 1996 15:37:39 -0400

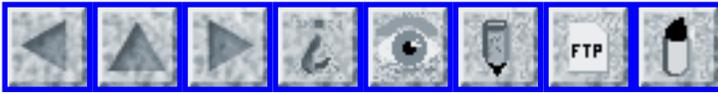
Since my comment questioning the 80% figure attributed to hate literature originating in Canada, I'd like to make some further comments in the hope of stifling further e-mail.

Has nobody but me stopped to consider what 80% means? To me, at least, this implies that out of <insert really big number> people connected to the Internet *worldwide*, Canada is implied to have the dubious honour of being Number One in providing hate literature to Germany, with Number Two placing a very distant second, whatever country that might be. Does this make sense?

Am I the only one wondering who took these stats, and what methodologies they used to collect them?

I thought one of the fundamental mandates for this newsgroup was to question the reliability of certain assumptions, especially if technology is involved. In fact, let me go so far as to say that one RISK in listening to rhetoric is to take as gospel when one throws around figures like "80% of Canadians," or "4 out of 5 dentists", when we pooh-pooh claims that use phrases like "a lot". Numbers and statistics somehow validate and ennoble what we might otherwise question. I had hoped that RISKS readers would be familiar with this.

Jim Carroll <pjcarrol@ca.oracle.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 18: Issue 14

Weds 22 May 1996

Contents

- [The National Research Council Study of National Cryptography Policy](#)
[Herb Lin](#)
- [Largest Computer Error in US Banking History: US\\$763.9 BILLION?](#)
[Dave Tarabar](#)
[David Kennedy](#)
- [Credit Lyonnais Fire](#)
[Boyd Roberts](#)
- [Gov't computer break-in in Australia](#)
[David Kennedy](#)
- [Computers facilitate foolishness](#)
[Mark Seecof](#)
- [Another Netscape Bug US\\$1K](#)
[David Kennedy](#)
- [Screensaviour?](#)
[Matthew P Wiener](#)
- [The risks of calling 800 numbers?](#)
[Rob Slade](#)
- [12am: noon or midnight?](#)
[Ken Knowlton](#)
- [The `pound' sign](#)

[Donald Mackie](#)

● [Prompt bus sign](#)

[Donald Mackie](#)

● [Addendum to my tirade on bad numbers](#)

[Bob Frankston](#)

● [When your last name's also a first name ...](#)

[Scott Alastair](#)

● [Number cruncher derides numbers](#)

[Bertrand Meyer](#)

● [Call for Participation - SEI Conference on Risk Management](#)

[Carol Biesecker](#)

● [Info on RISKS \(comp.risks\)](#)

⚡ **The National Research Council Study of National Cryptography Policy**

"Herb Lin" <hlin@nas.edu>

Wed, 22 May 96 13:54:00 EST

Please post this message widely

I am writing to let interested parties know about the imminent release of

the NRC's study of national cryptography policy. If all goes well, we

hope to release it on May 30, 1996. However, prior to that time, we won't

be able to comment on its contents.

For current information on release, visit the web site

<http://www2.nas.edu/cstbweb/220a.html>

When you visit that site, you'll have the opportunity to be put onto a mailing list so that we can inform you by e-mail when the report is available in print and/or electronically, as well

as any public events associated with the report (e.g., public briefings).

Herb Lin
Cryptography Policy Study Director
Computer Science and Telecommunications Board
National Academy of Sciences/National Research Council
202-334-2605

⚡ Largest Computer Error in US Banking History: US\$763.9 BILLION?

Dave Tarabar <dtarabar@systemsoft.com>
Mon, 20 May 1996 09:57:54 -0400

Approximately 800 customers of the First National Bank of Chicago were surprised to see that their balances were \$924 million more than they expected last week. The cause was the traditional ``change in a computer program''.

According to The American Bankers Association, the total of \$763.9 billion was the largest such error in US banking history. Do the RISKS Archives agree?

[Source: an AP story in **The Boston Globe**, 19 May 1996.]

Dave Tarabar SystemSoft Corp. 2 Vision Drive Natick, MA 01760
dtarabar@systemsoft.com 508 647-2952

[Yes. PGN]

⚡ Largest Computer Error in US Banking History: US\$763.9 BILLION?

David Kennedy <76702.3557@CompuServe.COM>

22 May 96 08:24:13 EDT

When Jeff Ferrera and Cindy Broadwater checked their checking balance at the First National Bank of Chicago, the automated voice gave it as \$924,844,208.32. More than 800 other folks had similar stories to tell. The sum total for all accounts was \$763.9 billion, more than six times the total assets of First Chicago NBD Corp. The problem was attributed to a ``computer glitch''.

[Source: AP US & World, 18 May 1996, By MARIO FOX, Courtesy of Associated Press News via CompuServe's Executive News Service. PGN Abstracting]

Credit Lyonnais Fire

Boyd Roberts <boyd@france3.fr>

Wed, 22 May 96 15:13:13 PST

I'm not sure how widely this was reported, but the head office of the Credit Lyonnais (a bank) in Paris (8e, rue du Quatre Septembre) had a major fire a few weeks ago. I forget the date, but it was a Saturday and the fire burned for quite a while. The investigation is proceeding, but my source of information has some things to say that may be interesting to RISKS readers:

1. The VMS machines in the building were part of a cluster that was replicated remotely.

So far so good.

2. There appears to have been no sprinkler system or fire doors

in the building. I've seen it, from the outside, and it's more

or less gutted.

Asking for trouble?

3. The UNIX machines were backed up daily, except for Fridays which

was done on Sunday. These machines were backed up to tape and

it appears that the tapes stay in the machines until just before

the next backup is done. Remember, the fire was on saturday.

24 hour operations are not that expensive. Courier the tapes

offsite, after they've been written. Offsite parallel operations?

4. On the Saturday the UNIX machines had the tapes for Thursday night

still loaded. They had not yet been put in the fireproof safe and

the backup of Friday's data had not commenced.

Backup your data ASAP, preferably to a remote site across a

network. If the tapes have to stay on site, put them in the safe.

5. In the middle of the _fire_ someone realised this small problem and

while the fire was still burning the tapes were rescued from the

UNIX machines and from the fireproof safe.

I wonder who volunteered?

6. Apparently the fireproof safe was not deemed to be waterproof or taking the tapes during the fire was deemed a better choice than maybe getting them later.

Water follows fire.

7. From the news reports it appeared that there was also some concern over whether safe deposit boxes (in the basement?) were waterproof.

All of this is unconfirmed, but I think my source is ok.

BTW: I bank with the Societe Generale.

Boyd Roberts
fr

boyd@france3.

Gov't computer break-in in Australia

David Kennedy <76702.3557@CompuServe.COM>
22 May 96 08:24:11 EDT

Courtesy of Australian Associated Press via CompuServe's
Executive News
Service:

QLD: THIEVES RAID GOVERNMENT BUILDING

Australian Associated Press 5/18/96 6:21 AM

Copyright 1996 The Australian Associated Press.

>> BRISBANE, May 18 AAP - Computer thieves raided one the
>>Queensland government's most sensitive buildings today,
>>ransacking three floors and dismantling around 55 computers,
>>police said.
>> A spokesman for Premier Rob Borbidge said the

>>break-in at the executive building annexe in George Street had
>>prompted a review of security at all government buildings.

o About 55 computers were taken apart and the HD and memory removed.

>> The spokesman for Mr Borbidge said the break-in in the
>>sensitive treasury area did not appear to be politically motivated.

[DMK: "Appear?" Kinda depends on what data "appears" on those
Hard Drives
doesn't it?]

[DMK#2: Murphy's Laws of Combat #14: When you secure the area
be sure to let
the enemy know.]

Dave Kennedy [CISSP] Information Security Analyst, National
Computer Security
Assoc.

⚡ Computers facilitate foolishness

Mark Seecof <Mark.Seecof@latimes.com>

Sun, 19 May 1996 13:44:01 -0700

I saw a demonstration of modern computer-voice-recognition s/w
tied to modern
ideographic text-processing software. It appeared to me to work
pretty well
(given that I didn't understand the language involved).

Even a few years ago, it appeared that the "information age" was
generating
forces which would push people away from ideographic writing
systems. Most
intellectual work would be supported by computerized systems
running on

alphabetic text; ideographic processing when available was costly, awkward, and slow. Furthermore, hardly anyone could program his computer (in the general sense) using ideograms. Though people using different alphabets could exchange information fairly easily, ideographic data was not very portable.

These forces seemed progressive. Alphabetic writing systems are much more convenient for most purposes than ideographic ones. Worse, cultures using ideographic systems force their young to spend tremendous amounts of time and effort memorizing ideograms--time which they could otherwise devote to productive or entertaining activities. Ideographic systems are bad for people with poor visual memories; though they may be capable of intellectual work, they find themselves crippled by their obdurate writing system.

But now computer advances (not unanticipated) will relieve some pressures which worked to push people away from ideographic systems. The tedium of penmanship will go away. Recognition of ideograms for programmatic purposes will become widely available. Most computer systems will become able to process and display ideographic text.

I fear that the usual forces of reaction and inertia which operate to maintain the cultural status quo may overpower the diminished forces of progress. Even though ideographic writing systems are demonstrably counter-productive, the slow-to-accrue benefits of abandoning them may never outweigh the instantaneous costs of doing so in the minds of adult (already

ideographized)
decision-makers.

Advances in computer systems will enable us to avoid advances in our "human systems." Heck, it's worse than "will enable us to avoid advances." It's more like "will actively retard us..."

Mark Seecof <marks@latimes.com>

⚡ Another Netscape Bug US\$1K

David Kennedy <76702.3557@CompuServe.COM>
22 May 96 08:24:09 EDT

Courtesy of the Dow Jones News Service via CompuServe's
Executive News Service

Princeton Team Finds Bug In Part Of Netscape Program
Dow Jones 5/20/96 6:02 AM

From The Wall Street Journal
>> MOUNTAIN VIEW, Calif. -- Netscape Communications Corp. said a
>>team of Princeton University computer sleuths found another bug
>>in the company's popular Internet browser, but said the flaw
>>has been corrected and no information was lost or damaged.
>>Jeff Trehaft, Netscape's director of security, said the bug was
>>buried "deep in the source code" of its Navigator browser, and
>>that it was so esoteric that only experts searching for months
>>could find it. The bug was found in Navigator versions that
>>support Sun Microsystems Inc.'s Java computer language.

o Third bug identified by the team. This one found by Thomas Cargill, a consultant.

o Netscape delivered a fixed version within 24 hours. Cargill still gets the \$1000 reward.

>> Mr. Trehaft added that Navigator is safe. "This product has
>>been out almost a year and only a few bugs have been found, and
>>as far as we know there's been no damage," he said.

Dave Kennedy [CISSP] Information Security Analyst, National
Computer Security
Assoc

[John Markoff had an article on this topic (See also [RISKS-18.13](#))

in *The New York Times*, Saturday 18 May 1996.]

⚡ Screensaviour?

Matthew P Wiener <weemba@sagi.wistar.upenn.edu>

Sun, 19 May 96 19:11:19 EDT

The 17 May 96 FORWARD (an American Jewish interest weekly newspaper), page 5, has a brief article about a Jewish CD-ROM put out by the Jewish Publications Society that had a Christian gospel screensaver by mistake.

JPS is a large Jewish publisher. But they had never done a CD-ROM before, so they asked Logos Research Systems, a leader in Christian software products, to do the scutwork. Apparently the screensaver was added in at the last minute, and since there were no instructions regarding it, the generic Logos screensaver was packaged in, and presumably nobody beta (beth?) tested it.

JPS and Logos are now splitting the cost of replacing hundreds of CD-ROMs already sold, and are pulling off those on the shelves.

-Matthew P Wiener (weemba@sagi.wistar.upenn.edu)
The Wistar Institute of Anatomy and Biology

⚡ The risks of calling 800 numbers?

"Rob Slade" <roberts@mukluk.hq.decus.ca>
Tue, 21 May 1996 18:10:14 EST

Ah, the things we don't know about 800 service. Like: Call(er ID) Blocking doesn't work: the owner of the 800 number gets your number anyway.

And now this:

```
>From: Abram the spammer
>Newsgroups: alt.books (no less!)
>Subject: HAIR LOSS?....MINOXIDIL USERS?
>
>Now available in the U.S.  XXXXXXXXXXXX AND XX-XXX XXXX.
>Japan and West Germany's leading treatment for thinning hair.
>2.5X more effective than minoxidil. Featured on CNN, NEWSWEEK,
>NEW YORK TIMES. DOCTOR recommended. For FREE information,
>please call 1-800-555-XXXX
```

Ah, but here's the cute part:

```
>*PLEASE NOTE THAT ANY CALLS NOT PERTAINING TO INFORMATION
REQUESTS
>WILL BE AUTO-BILLED TO ORIGINATING NUMBER UTILIZING
>LONG DISTANCE SURCHARGES.
```

In other words, he is quite willing to spam news, but he doesn't want anyone spamming his 800 number in retaliation.

Of course, he could just be bluffing. Any telco people know if this is available?

⚡ 12am: noon or midnight?

<KCKnowlton@aol.com>

Tue, 21 May 1996 22:02:15 -0400

There are compelling reasons to consider "12 am" to mean noon, as in the hour-by-hour sequence 10 am, 11 am, 12 am. But just as compelling is the minute-by-minute sequence 12:00 pm, 12:01 pm, 12:02 pm. People generally duck (actually clarify) the issue by saying "12 noon" and "12 midnight." Another dodge is to make rules and laws go into effect at such times as 12:01 am.

But
is there a more or less universally understood meaning of 'am' or 'pm' as applied to exactly 12? If there isn't, what should it be?

The truly logical answer to this, of course (try to get this one through Congress) is to replace 12 by 0: there's no confusion about

what 0 am and 0 pm would mean. Not to me anyway.

Ken Knowlton

[Lots of folks around the world solve this by going from 00:00 through 12:00 to 23:59 each day. Who needs am, p, n, and m?

So, perhaps a correct answer to the Subject line is
neither. PGN]

⚡ The `pound' sign

Donald Mackie <donald@iconz.co.nz>

Tue, 21 May 1996 22:22:53 +1200

The pound sign `#' is often used as shorthand for the word `fracture' by medical staff from the UK and other countries. For example, "Mrs

Smith has
a # radius and ulna".

Our hospital computer systems move data from one system to another. If Mrs Smith's diagnosis is entered as above on the administrative system and then her information is called up from the pathology system the diagnosis appears as "=A3 radius and ulna".

Of course, the same problem may occur in transmission of this message. The pound or hash sign is replaced by the stylised L used to designate the pound sterling (currency).

RISK: the patient's arm may be more valuable to pathology than anyone else.

Donald Mackie FANZCA FRCA=20 Middlemore Hospital, Auckland, New Zealand
ph +64 9 276 0168 fax +64 21 785 378

⚡ Prompt bus sign

Donald Mackie <dona1d@iconz.co.nz>
Tue, 21 May 1996 22:22:58 +1200

Our local buses have electronic signs on the front, rather like those used for airport departure boards. The sign shows the destination of the bus and scrolls through stops it is yet to make. As the bus passes each stop it is removed from the list.

Yesterday I saw a bus apparently destined for

>:run64

I suspect the driver needed to hit <enter> just one more time.

Donald Mackie FANZCA FRCA Middlemore Hospital, Auckland, New Zealand

ph +64 9 276 0168

fax +64 21 785 378

✶ Addendum to my tirade on bad numbers (... Births, [RISKS-18.10](#))

<Bob_Frankston@frankston.com>

Tue, 21 May 1996 12:58 -0400

I'm watching CNN as background noise and they are touting the use of Astrology for investing. The problem is just another illustration of how difficult it is to get straight information to form ones one judgment. They noncritically report that three successful predictions including the Gulf war. There is not an iota of incredulousness -- not only does the reporter not do fact checking (what is a prediction?) there isn't even the idea of checking to see if there is any significance against the larger set of predictions. Astrology is an obvious target but there is no reason to assume any of the other reports are any better researched. Reminds me of the great Dilbert strip where the Boss is determined to track down the miscreants since a full 40% of the sick days were on Monday or Friday. But it's not just innumeracy.

Lest we be smug (whoever "we" are) the same naivete appears in assuming that

one can simply design a system and deploy it without a continual learning and refinement cycle. (formerly known by its denigrated name of "maintenance").

⚡ When your last name's also a first name ...

"Scott Alastair (Exchange)" <ScottA@logica.com>

Mon, 20 May 1996 09:07:24 +0100

I have the misfortune to have both an unusual first name (Scottish Gaelic) and a last name which passes muster as a first name in most, if not all, of the English-speaking parts of the world.

Our Microsoft Exchange mail system stores names as <last name> <first name>.

So I am seen by the world as "Scott Alastair" when Exchange puts its own header at the top of mail messages I send. Despite many variations - of increasing literary violence - of signature most (about 75%) of my Internet email is addressed, "Dear Scott".

I am told that names are stored as <last name> <first name> because, for example, the sender can type "Scott Al" and Exchange will match my name automatically without the poor sender having to spell "Alastair" correctly.

A fix has been considered - storing the names as <last name>, <first name> - but was rejected as too risky because people would forget the comma.

So I can't win! If an Alistair Scott (note the spelling, which is actually more common than my spelling) joins,

I'm Alastair Scott; MS Exchange calls me Scott Alastair
scotta@logica.com +44 (0)171 446 4899 Logica UK Limited

[Not to mention the confusion between Li Gong and Gong Lim
although
the former name has been Westernized. PGN]

⚡ Number cruncher derides numbers

Bertrand Meyer <bertrand@eiffel.com>

Sat, 18 May 96 14:19:08 PDT

A story in the 29 Apr 1996 issue of Web Week, a magazine devoted to the World-Wide Web, describes new developments in the controversy between Nielsen Media Research and a group of academics from Vanderbilt and North Carolina, who criticized an earlier Nielsen study as overstating Internet usage in the US and Canada.

The magazine quotes the following from David Harkness, senior VP of Nielsen Media Research: "What doesn't matter now, in my opinion, is how many users there were in August of last year, because the Internet is growing so fast. The Internet is not being served by this debate".

The last comment may cause anyone who has forked out \$5,000 - what the magazine says it takes to buy a copy of the Nielsen report - to raise an eyebrow or two. Are we to understand that the purpose of such a study is to "serve the Internet", that is to say cheer up everyone in the Internet

industry by reporting good news, rather than provide a snapshot of the reality?

But the most interesting part remains the first sentence in Mr. Harkness's comment. If I understand properly: let's not quibble about minor differences between the two studies (a mere 8 million people - or actually 20 million, making the result more than 100% off target, if you compare Nielsen's "Internet access" numbers with the academics' estimates of actual Internet use!); we all know the Internet is expanding by leaps and bounds.

Which of course brings up the whole question of why we should trust Nielsen's numbers any more than Mr. Harkness seems to. For example, according to his study, 1.51 million people have used the Web to make a purchase. Even if you bought the report, better double-check before making a major policy decision based on such statistics.

-- Bertrand Meyer, ISE Inc., Santa Barbara, <bertrand@eiffel.com>
Posting applying the SELF-DISCIPLINE rules, see <http://www.eiffel.com/discipline>

✶ Call for Participation - SEI Conference on Risk Management

Carol Biesecker <cb@SEI.CMU.EDU>
22 May 1996 18:43:34 GMT

Call for Participation
Software Engineering Institute (SEI) Conference on Risk
Management:

acquisition, programs, projects, systems, and software

Managing Uncertainty in a Changing World

Hotel Cavalier

Virginia Beach, Virginia

April 7-9, 1997

In today's world of downsizing and reengineering, you're moving into uncharted territory. You've been asked to acquire and develop systems with less money, and said, "I can do that." You've been asked to succeed with shorter schedules, and said, "I can do that." You've been asked to use fewer people, and said, "I can do that."

So, how can you do that?

You need to improve your ability to acquire systems, to proactively manage your resources, people, schedules, and budgets--to predict and avoid problems before they occur. You must rapidly integrate, under controlled conditions, the acquisition of complete systems providing end users with predictable system performance. You need to determine which risks are more critical to the success of your program to make effective use of scarce resources. You need proven methods and techniques as well as suggestions for advanced capabilities.

Acquisition practices and risk management are being implemented and improved throughout the government and industry. To maintain your competitive edge in this uncertain world, you need effective acquisition and risk management practices. This conference is a way to find out what's going on and what's

applicable and useful to you.

The SEI Conference on Risk Management will provide a forum that brings together the government, industry, and academic managers, practitioners, change agents, and researchers using and exploring risk management and acquisition. The conference will provide a unique forum for exchanging ideas and experiences with experts and professionals who practice or study acquisition and risk management. This is a tremendous opportunity to increase your awareness and to advance your knowledge and skills by being exposed to the latest methods, tools, and techniques, and some of the best practices in the field of system development and acquisitions. Managers will find the means to improve their ability to make informed decisions and to gain better control of their project's cost, schedule, and technical contents. Practitioners will find the ways to increase awareness of risks and their ability and skills to avoid or mitigate them. Both development and acquisition professionals will gain insight from the experiences of leading experts and professionals, learn about the latest developments and technological issues, and learn how to manage uncertainty in a changing world.

The SEI Conference on Risk Management will feature keynote speakers, distinguished presenters, selected presentations from invited speakers, panel discussions with experts and professionals, and exhibitors. It will also provide learning opportunities with hands-on tutorials and

opportunities to accomplish work to advance the practices of acquisition and risk management through mini-workshops. The conference will further provide value for different audiences such as managers and practitioners, beginners and advanced professionals, or development and acquisition professionals through separate tracks for presentations and panels. Opportunities to mingle with people who have similar interests will be provided through birds-of-a-feather sessions.

The Hotel Cavalier in Virginia Beach provides beach-side accommodations. The Virginia Beach area is convenient to Washington, D.C. and offers golfing, deep-sea and freshwater fishing, tennis, hiking, historic dwellings, museums, shops, and restaurants. The Norfolk International Airport serves the Virginia Beach area with more than 200 flights daily to all major hubs and most major cities. The oceanfront is a 20-minute drive from the airport.

Important Dates

September 19, 1996: deadline for submitting papers and workshop proposals

October 17, 1996: deadline for mailing acceptance notification to participants

January 24, 1997: deadline for submitting camera-ready materials

For more information about the conference, contact--
SEI Customer Relations
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213-3890
Phone 412 / 268-5800
FAX 412 / 268-5758
Email customer-relations@sei.cmu.edu

World Wide Web <http://www.sei.cmu.edu>

For more information about vendor exhibits, contact--
Heather Stupak, as above, with Phone 412 / 268-1587, FAX 412 /
268-5758
Email hstupak@sei.cmu.edu

[Truncated for RISKS. 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 18: Issue 15

Friday 24 May 1996

Contents

- [U.S. National Research Council Study of National Cryptography Policy](#)
[Herb Lin](#)
- [TILT! Counterfeit pachinko cards send \\$588M down the chute](#)
[Peter Wayner](#)
- [Security by accident](#)
[Douglas W. Jones](#)
- [A few little UK vignettes ...](#)
[Les Hatton](#)
- [The Power of Alta Vista](#)
[Rachel Polanskis](#)
- [Senate Hearing #1 on Information Security: GAO Report issued](#)
[David Kennedy](#)
[Ted Lee](#)
[Alan Tiganelli](#)
- [Frequently used German passwords](#)
[Martin Virtel](#)
- [The risks of calling 800 numbers?](#)
[Bob Blakley III](#)
- [Re: pornography on net: real risk?](#)
[Bob Morrell](#)

- [Re: Non-universal names for symbols](#)
[Angus Duggan](#)
 - [Society and the Future of Computing Update](#)
[Rick Light](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✈ U.S. National Research Council Study of National Cryptography Policy

"CRYPTO" <crypto@nas.edu>
Fri, 24 May 96 15:20:00 EST

The Computer Science and Telecommunications Board (CSTB) of the National Research Council (NRC) has completed a congressionally mandated study of national cryptography policy. The final report, *Cryptography's Role in Securing the Information Society*, will be released to the public on May 30, 1996 at a public briefing. Many of the authoring committee members will attend.

The public briefing will take place in the Main Lounge of the National Press Club, 14th and F Streets, N.W., Washington, D.C., from 1:00 PM to 3:00 PM, on Thursday, May 30, 1996. Committee members will respond to questions from attendees, and a limited number of pre-publication copies of the report will be available at that time. By the close of business on May 30, a summary of the report will be made available through <http://www2.nas.edu/cstbweb>; the full publication will be made available when final printed copies of the book are available (probably around the beginning of August).

The committee also intends to conduct a second public briefing on the report in Menlo Park, California at SRI International. The briefing will be held in the Auditorium of the International Building from 10 to 11 am on Wednesday, June.5. The address is 333 Ravenswood Avenue, Menlo Park, California, 94025. For more information about the briefing at SRI, contact Alice Galloway at 415-859-2711 (alice_galloway@qm.sri.com).

If you have suggestions about other places that the committee should offer a public briefing, please let me know (crypto@nas.edu or 202-334-2605).

If you wish to be kept informed of various other public activities regarding dissemination of this report, you can sign up for an e-mail list by visiting the web page [ttp://www2.nas.edu/cstbweb/notifyme.html](http://www2.nas.edu/cstbweb/notifyme.html).

I apologize to you for the short notice on this invitation, but hope that you will be able to attend.

Herb Lin
Senior Staff Officer
Study Director
CSTB/NRC Study of National Cryptography

Policy

🔥 TILT! Counterfeit pachinko cards send \$588M down the chute

Peter Wayner <pcw@access.digex.net>

Thu, 23 May 1996 08:17:19 -0400

The **Wall Street Journal** of 22 May 1996 (A18) reports that two

Japanese

firms lost about 55 billion yen when criminals counterfeited the stored money cards that they manufactured. These cards are used to pay for pachinko games, but you can get refunds wired to an account if you cash in a card. If my memory serves me correctly, there is a certain amount of skill involved. If you play well or are lucky, you might even add money to the cards. But I'm not sure about this detail. In any case, the people with the counterfeit cards could get refunds when they didn't pay for the original card.

The Journal mentions three interesting details. First, the cards were pushed by the police as a means to track the flow of cash and stop money laundering. Obviously, there wouldn't be these losses if they could really track the flow. Second, the convenience of the new cards initially boosted profits because it was so much easier to play with the cards that automatically kept track of your money. Finally, the Journal reported that there are 18,244 pachinko parlors in Japan.

✶ Security by accident

Douglas W. Jones <jones@pyrite.cs.uiowa.edu>
22 May 1996 21:29:50 GMT

I serve on the Iowa Board of Examiners for Voting Machines and Electronic Voting Systems, and last Monday, we met to examine a new modem feature added to the already approved BRC Eagle mark-sense voting machine.

One question that came up immediately is that, given the fact that Iowa's current voting law bases the official canvass of votes on hand-delivered reports from each precinct, what value does a modem serve? The answer is trivial -- unofficial counts phoned in from the precincts are routinely used to compute unofficial totals that are then released to the public and press soon after the polls close. Right now, these totals are usually phoned in manually (or should I say, orally), but a modem in the voting machine can easily serve the same purpose.

An aside: Why the big push for instant results? Sure, the press wants fast access to the totals, and counties compete to see who can get their totals in first, but we'd probably be better off as a nation if there was a news blackout on vote totals until the day after!

It seems likely that electronic reports will soon be used to formulate the official canvass. Currently, the canvass is done by reading the tapes printed out by computerized voting machines and manually (or with the aid of calculators and computers) tallying the votes; this introduces a needless source of error.

Because of this, we decided to examine BRC's new modem feature with an eye towards the possible incorporation of direct electronic vote total reporting into the official canvass. An obvious question that comes up in this context is, how secure is the system. BRC's written answer to this question

(one I submitted in writing in advance) boiled down to:

- 1) BRC uses a proprietary protocol
- 2) The central host, on receiving a report by modem, gives no feedback until it receives the whole packet of vote totals.
- 3) The central host demands that each voting machine present the correct 8 digit ID code before it accepts a record of votes cast.
- 4) Each voting machine has a 4 digit ID code that is padded to 8 digits to make the required ID code.
- 4) Failed connection attempts are logged and flagged on screen at the central site.

Needless to say, the idea of a 4 digit PIN being sufficient didn't impress me, nor did the idea of security through obscurity. The lack of feedback helps security, but in a jurisdiction with hundreds of voting machines, the 4-digit code space will be pretty full. As a result, we had an interesting discussion of the security issue; this ended when Herb Deutsch from BRC, said the following, almost in passing (quoted from memory):

"Oh, by the way, we also include a timestamp in the data and verify that it is right. It's the time the PROM customizing that particular voting machine for that particular election was burned, and it's accurate to the IBM PC clock precision. I didn't even think of it as a security feature, but I guess it is."

Not only hadn't he thought of this feature as being part of the security of modem-based vote reporting, but he then went on to explain why the

software included a feature to allow a total with the wrong timestamp to be accepted despite a timestamp mismatch error. There was no similar way to override a 4-digit PIN mismatch.

We approved the machine (Of course, we also tested other things, for example, by injecting line noise on the phone line while totals from a test election were being reported). We also made the administrative recommendation that, despite the fact that vote totals delivered by modem are currently not official, central election workers should not override timestamp mismatches or other overridable error conditions without explaining why in the presence of witness from at least two political parties (this is the usual precaution required for all manual vote processing steps).

If electronically reported vote totals become part of the official canvass, we concluded that we'd like to see some of the time spent manually tallying the canvass spent auditing the machine computed results. Right now, in Iowa, no recounting of votes is allowed unless there is a call for a recount. As currently set up, this prevents reasonable auditing steps such as recounting randomly selected precincts or post-vote testing of randomly selected voting machines. We concluded that these kinds of tests should be routine and should be completed prior to the certification of an automatically computed purely electronic canvass.

We also concluded that, someday soon, we'd like to see standards

for
electronic vote reporting from machine to central counting
location.
Security through obscurity isn't desirable, and cross-vendor
compatibility
is important! Voting machines are expensive, and a standard
would
significantly simplify incremental replacement of old voting
machines.

Doug Jones jones@cs.uiowa.edu

✶ A few little UK vignettes ...

"Les Hatton" <les_hatton@prqa.co.uk>
23 May 1996 13:44:15 +0000

1) Election results. The BBC operates a magnificently indulgent
set of
computer graphics for predicting the various results of
elections. In an
interview on BBC News Extra on 3 May 1996, its presenter, Peter
Snow, was
asked if there were ever problems. "Oh yes", he replied. "For
example, in
the Dudley (a Midlands town) bye-election, the swing away from
the (ruling)
Conservative government was so large that the entire screen went
blank
because the programmers had not allowed for the Conservatives
having no
seats (i.e. elected representatives)".

2) Airline entertainment systems. During a single flight from
Singapore to
London experienced by myself in April 1996, the Singapore
Airlines inflight
entertainment system, "Krisworld", was rebooted twice in the
first two
hours, numbered its video channels with the rather eccentric

numbering
system, 1,2,3,4,5,6,48,8,... and then lost the numbers
completely for a
while so the video channel had to be guessed. This is a regular
occurrence
according to my colleagues.

3) Taxation. It was recently reported in the UK (April 1996 on
www.netaccountants.com) that "A VAT Tribunal has shown the
Customs & Excise
VAT computer was incorrectly calculating VAT surcharges for late
filing of
returns. Customs have estimated that about 90,000 default
surcharges were
too high and have said that the way that the computer was
programmed means
that Customs cannot identify the businesses that have been
overcharged !"

Les Hatton, Ph.D. C.Eng, Director of Research & Engineering,
Programming
Research Ltd, England les_hatton@prqa.co.uk +44 (0) 1 932 888
080

The Power of Alta Vista

Rachel Polanskis <r.polanskis@nepean.uws.edu.au>

Thu, 23 May 96 19:44:35 1000

This is about a discovery I made with Alta Vista the WWW search
engine, and
its robot "scooter".

The system I hit on had a high port of 8000 and I accessed it
via Netscape 1.1N
for the PC, through Alta Vista...

I can not believe what happened to me, and it has elicited a bit
of interest

around the place. I hope I never see it again!

Here is the article I posted:

Hello everyone.

I thought I might share with you an experience I had today while searching the Internet for information on some programming topics.

I used Alta Vista to do a search on some programmers' libraries, for my home UNIX network.

The software I wanted is actually commercial, and not freeware, and is unavailable except by purchasing it.

Imagine my surprise when Alta Vista returned in its little search screen:

```
"Directory of /lib"
```

Hmmmm.....

I proceeded to follow this link, hoping I might have hit on a public archive of software made available on the public domain, as the OS I wanted it for is basically obsolete.

I was even more interested when I saw several system libraries scroll by on my screen...

A quick check of the root home page of the system (i.e. just the domain name without a path to files) brought back the following:

```
> Index of /
>   Name                Last modified      Size  Description
>
>   bin/                 15-May-96 14:20    -
>   boot                 17-Nov-93 00:12    101K
```

[...]
>33 files

To the uninitiated, this is the *root filesystem* of the UNIX host I was visiting via netscape.

I changed directory to /etc and was amazed to see everything available to me.

I clicked on /etc/motd and that was enough to tell me I could have had the password file had I wanted to.

I mailed the site's admin and postmaster telling them of the security breach.

The site is now offline since I checked tonight.

Now, people - that is what Alta Vista can do on an unsecured UNIX server.

Their whole machine - user private directories and everything - even files made read by the system only were publically available for anyone to download.

Had I been malicious, I could have downloaded the password file, cracked it with crack, logged in as root, and deleted the syslogs and no one would have been the wiser to my presence, at least for a while anyway.

There is no moral to this story - if there was one it would be something like: "You Are Being Indexed" - if you do not take care.

Be careful of what you put on your computers.
If there is a hole, Alta Vista will find it.
And it is damn good at indexing Hard Disks.

The site was indexed by Alta Vista's robot more than a week ago...

Rachel Polanskis, Kingswood, Greater Western Sydney, Australia
grove@zeta.org.au r.polanskis@nepean.uws.edu.au

🔥 Senate Hearing #1 on Information Security: GAO Report issued

David Kennedy <76702.3557@CompuServe.COM>
23 May 96 13:40:31 EDT

Courtesy of Associate Press via CompuServe's Executive News Service

Copyright 1996 The Associated Press. All rights reserved.

Computer Security

By JIM ABRAMS, Associated Press Writer

>> WASHINGTON (AP) -- Hackers infiltrate Pentagon computers
>>more than 160,000 times a year, threatening "catastrophic
>>damage," but the military rarely detects and seldom
>>investigates the interlopers, government investigators said
>>Wednesday. "At a minimum, these attacks are a
>>multimillion-dollar nuisance to Defense. At worst, they are a
>>serious threat to national security," the General Accounting
>>Office said.

o GAO repeated the DoD estimate of 250K attempts last year.

Testimony

highlighted it was an estimate, but also that in GAO's opinion
it was

probably more accurate of an estimate than anyone else's.

[DMK: The article states 65% of these were successful, but that
was not what

was in the testimony before the Senate. I watched the testimony
on CSPAN

last night (yes I do too have a life) and the testimony was that
DoD

estimates 250K attempts, and DoD's own testing had a success
rate of about
65%.]

>> The report, presented to the Senate Governmental Affairs

>>subcommittee on investigations, dealt with the more than 90
>>percent of Pentagon data that is unclassified. It nevertheless
>>could contain highly sensitive information on troop movements,
>>procurement and maintenance of weapons systems.

o Testimony included 120 countries (identity classified) have
or are
developing computer attack capabilities.

>> The report quoted the Pentagon as accepting that the
>>document fairly represented the increasing threat of Internet
>>attacks. Officers attributed some of the problems to poorly
>>designed systems or to the use of off-the-shelf computer
>>products without inherent security safeguards.

o Both the Senate testimony and the Pentagon spokesperson
highlighted
the issue is unclassified information and that classified
information was
secure. [Well, not quite... PGN]

>> Pentagon spokeswoman Susan Hansen also stressed that the
>>report focused only on unclassified transmissions between the
>>department and the outside world. Information on weapons
>>systems and other classified material was secure, she said. "We
>>have invested in those systems so they are not subject to those
>>attacks," she said, "but we are not taking lightly the
>>repetitive and constant attacks" on unclassified Pentagon
>>networks.

o Testimony include the Griffiths AFB penetration by the hacker
Datastream Cowboy in early 1994:

>> To avoid detection, the hackers went through international
>>telephone lines, passing ports in South America, Seattle and
>>New York to reach the Air Force computer. From there, they
>>broke into computer systems of NASA, Wright-Patterson Air Force
>>Base, defense contractors around the country and South Korea's
>>atomic energy center.

...

>> The report noted that the Defense Information Systems Agency
>>has conducted 38,000 attacks on Defense computer systems via
>>the Internet to see how well they are protected. The agency

>>gained access 65 percent of the time.
>> Of these successes, only 4 percent were detected by target
>>organizations, and in only 27 percent of those cases was the
>>detection reported to the systems agency.

Dave Kennedy [CISSP] Information Security Analyst, National
Computer Security
Assoc.

[The report is available from the Government Accounting Office,
GAO/AIMD-96-84, Information Security: Computer Attacks at
Department
of Defense Pose Increasing Risks. Cliff Stoll, Bob Anderson
of RAND,
and I were at the hearing, having been invited to testify.
However, our
testimony has been postponed because the Senate decided to do
a blitz
voting on 40 issues at 10 minute intervals, so the hearing was
cut short.
PGN]

🔥 Senate Hearing #1 on Information Security: GAO Report issued

Ted Lee <timplee@MR.Net>
Wed, 22 May 1996 16:07:51 -0600

... I have three questions: a) how did they
go about collecting such statistics, b) if the systems had
software good
enough to notice that they had been penetrated, why couldn't
they have
stopped the penetration, and c) how many successful or
unsuccessful attempts
were not detected? (Not that I have any idea how one would go
about getting
that number.) I will grant, for instance, that if the attack is
a password
attack where the search was done on another system on a copy of

the password
file one might not detect it until considerably after the fact,
but unless
the penetrators actually caused damage I would suspect any such
successful
attacks wouldn't be noticed at all (who bothers to look at the
"last login
time" notice, if there even is one?) -- the impression I have
(but one must
also question here how one would validate this) is that most
hackers don't
damage data, just look at it. I will also grant that intrusion
detection
systems (which can detect mosquito bites but not technically
competent
attacks) might work slowly enough as not to be able to stop an
attack in
progress, but I suspect that most of the systems involved (the
stories said
something about mass-marketed computers) don't have any
intrusion detection
installed.

I don't doubt the message (things are bad and getting worse);
what I do
doubt is whether there is any scientific validity to the
numbers. The
RISKS? a) an unnecessary amount of money will be spent on solving
a
non-problem, or b) the problem actually is real, but the flawed
nature of
the statistics will be questioned and the opposite will happen.

Dr. Theodore M.P. Lee Consultant in Computer Security PO Box
1718 MN 55345
tamplee@MR.Net Minnetonka, 612-934-4532

🚩 Senate Hearing #1 on Information Security: GAO Report issued

Alan Tignanelli <75453.2055@CompuServe.COM>

23 May 96 12:41:59 EDT

... The part that I found interesting was this quote (from the Pittsburgh Post-Gazette, by Nolan Walters of the Knight-Ridder News Service):

"A 16-year-old kid from the United Kingdom, with the computer nickname 'Datastream Cowboy,' used a common 486 SX desktop computer, with *only a 170-megabyte hard drive,* to break into the Rome Laboratory sytem..." (my asterisks for emphasis - AT)

Is it just me?? "Only a 170-megabyte hard drive??" Good thing he didn't have one of those fancy-schmancy 2-Gig drives - think of what kind of systems he could have broken into!!!! Yet another example of the uninformed writing for the uninformed.

Alan Tignanelli

✶ Frequently used German passwords

Martin Virtel <M.VIRTEL@BIONIC.zerberus.de>

Thu, 23 May 1996 10:46:40 +0100

RISKS readers are well aware the RISKS of frequently used (and thus easy to guess) passwords. For the record (and for those of you who run sites where German speakers have passwords), here is the "most popular passwords" list for German, as obtained by a computer magazine's (PC Welt Extra) survey and reproduced by AP in Sueddeutsche Zeitung, May 22nd 1996, p.12:

1. Passwort ("password", could also be spelled
<HTML>Paßwort</HTML>)
2. Pass (no translation)
3. Liebe ("love")
4. Sex (same)
5. Gott ("God")
6. Genie ("genius")
7. Hacker (same)
8. Geheim ("secret")

Next are names, of the users themselves as well as names of spouses and children. I wonder if there is anybody willing to comment something on "German character" due to the passwords Germans are choosing, or any similar lists for other languages leaving room for (risky) "national character" studies :-)

Martin Virtel

PS. Any occurrences of this message being held up by mail filters because of the fourth most popular password welcome.

✂ The risks of calling 800 numbers? (Slade, [RISKS-18.14](#))

Bob Blakley III <blakley@VNET.IBM.COM>
Wed, 22 May 96 19:47:42 EDT

There are risks associated with assuming you're smarter than the spammers.

Here the tactic is simple, regardless of whether auto-billing to originating callers is possible: spam this number from pay phones. They all dial 800 numbers (isn't it a regulatory requirement, like 911?), their

users are completely anonymous, and their operators would almost certainly not be held liable for charge-backs under this scheme.

Bob Blakley, IBM Austin, 11400 Burnet Rd. Bldg 903 Rm 7b-01
(blakley@vnet.ibm.com) FON 512 838-8133 t/1 678, FAX 838-0156 t/
1 678

✶ Re: pornography on net: real risk?

Bob <bmorrell@bgsm.edu>

Thu, 23 May 1996 11:05:19 -0400 (EDT)

In [Risks 18.13](#) (May 17, 1996) Simson L. Garfinkel said of his small ISP:

>

> ... we specifically block the alt.binaries groups. The principle reason

> that we do this is to conserve our bandwidth: receiving alt.binaries

> would require that we triple our off-island throughput.

^^^^^

Now, skipping the moral and legal points noted by Mr. Garfinkel, with which

I mostly agree, my main observation was this: is this what the internet

=really= is all about? This and other stories, some on RISKS suggest that

the search for soft and hard core porn make up the majority of internet

traffic. This is a very disheartening to those of us who wish the net to

thrive and realize its potential. The net will not thrive if its main

purpose is the exchange of pornography. Eventually society will recognize

its non-productive nature and abandon it. Indeed the predictions of the

collapse of the net, widely reported recently, addressed this perception that few real uses for the net had been found.

The risk? As more and more =quantitative= stories like Mr. Garfinkel's come to light, the size and scope of the net's "dirty secret" becomes apparent, commercial, scientific, and other interests will decide the net is a bad neighborhood to hang out in. If more ISP's took Mr. Garfinkel's stance, the =long term= interests of the net would be better served.

Bob Morrell bmorrell@bgsm.edu <http://pandoras-box.bgsm.edu/micro/tech.html>

✶ Non-universal names for symbols (Re: Mackie, [RISKS-18.14](#))

<angus@harlequin.co.uk>

Thu, 23 May 1996 10:19:37 +0100

There is another risk here, partly computer-related, which is that of using names for symbols which are not universally recognised. There was has recently been a long discussion on comp.fonts about the proper name for the '#' symbol. The concensus seemed to be that while US readers recognised the name 'pounds' for this symbol, UK readers did not. They tended to know the symbol by the names 'hash', 'square', or 'sharp'. This name by which this symbol is known appears to be related to the context in which it is encountered; other names included 'nittle' (apparently used in the building trade) and 'octothorpe'

(used by some phone companies).

We use symbols in computing which are not part of normal everyday life; the risks are that as more non-technical people use computers, there will be more mistakes and confusion stemming from the wrong symbols being used, or symbols being used inappropriately.

Angus Duggan, Harlequin Ltd., Barrington Hall, | INET:
angus@harlequin.co.uk
Barrington, Cambridge CB2 5RG, U.K. | FAX: +44(0)1223 873873

⚡ Society and the Future of Computing Update

Rick Light <rxl@lanl.gov>

Wed, 22 May 1996 16:14:26 -0600 (MDT)

Society and the Future of Computing '96
June 16-19, 1996, Snowbird, Utah, USA
<http://www.lanl.gov/SFC>

All conference information and the registration form are available through the Web site (<http://www.lanl.gov/SFC/96/>).

Any questions or comments you might have may be addressed to sfc96@lanl.gov.

[See [RISKS-18.07](#) for earlier announcement. 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 18: Issue 16

Saturday 1 June 1996

Contents

- [Xerox machine caused nuclear power plant emergency halt](#)
[Magnus Ihse](#)
- [NY Air Route Traffic Control Center computer failure](#)
[Peter Ladkin](#)
- [US Charges Man Planned to Kill 4,000 Travelers](#)
[PGN](#)
- [Assumptions about assumptions at 12](#)
[Ken Knowlton](#)
- [Re: TILT! Counterfeit pachinko cards ...](#)
[Chiaki Ishikawa](#)
- [Timing out e-mail -- "kidsciencenet" spam](#)
[Laurence Brothers](#)
- [Access to psychiatric records](#)
[Bob Frankston](#)
- [Smartcards and medical data standards](#)
[Peter Bray](#)
- [Re: Largest Computer Error in US Banking History?](#)
[Louis Koziarz](#)
- [Risks of Statistics in RISKS-18.13](#)
[Frank Fay](#)

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

Xerox machine caused nuclear power plant emergency halt

Magnus Ihse <d95-mih@nada.kth.se>

Thu, 30 May 1996 13:16:56 +0200 (MET DST)

One of the Swedish nuclear reactors, Ringhals 4, was automatically shut down during a routine safety check. The last part of the instructions fed into the computer was missing, and when the computer safety system noticed that the instructions were incomplete, it shut down the reactor.

So far so good, but why were the instructions incomplete? The Xerox machine used to copy the instruction sheet did not include the complete page, and no one (except the computer) ever noticed that the instructions were incorrect.
(Source: TT)

The risk is obviously that no system is completely fool-proof. I doubt anyone ever thought about the correctness of the Xerox machines as part of the nuclear power plant safety system. No matter how detailed you planned the security system, there will always be some part that could fail. In this case, nothing serious happened because the computer detected the error. However, this -- or similar incidents -- could happen again, and next time maybe the error would not be detected.

Magnus Ihse, Computer Science student, Royal Institute of Technology, Sweden

✈ NY Air Route Traffic Control Center computer failure

Peter Ladkin <ladkin@TechFak.Uni-Bielefeld.DE>

Thu, 23 May 1996 21:28:10 +0200

The NY ARTCC computer (7 years old) lost significant service capability ('failed' said the NYT Service's Matthew Wald on 21 May 1996) twice on the evening of Monday 20 May; the first time for 23 minutes, and the second time for about an hour, one hour later. The NYTS reported (International Herald Tribune, Thurs 23 May 1996 p2) that it was 'running normally' Tuesday as technicians tried to figure out the problem. The FAA is wondering about the new software installed four days earlier.

'The office, the New York Air Route Traffic Control Center, handles high-altitude and long-distance traffic over New York, Connecticut, New Jersey, Pennsylvania and part of the Atlantic Ocean.' (Wald, NYTS, 21 May 1996)

There followed the usual: a fail-safe return to older, more inefficient air traffic control procedures, leading to a lower traffic saturation limit and thus mean delays in departures of about an hour at major airports in the area; an increase in the work load of controllers; a deficit of safety-related information, including 'automatic conflict alert'.

I note that a deficit of safety-related info does not necessarily lead to a reduction in safety: one increases safety margins and pays careful

attention (which might even increase safety for the short periods involved).

These older procedures worked tried and true for decades. Risks might increase were an ARTCC system to suffer a service reduction at a time at which there were more aircraft in the system than the saturation limit for the reduced level of service. Aircraft in the air already under control do not just go away, however one can delay entry into Center control by delaying aircraft ready for departure and diverting flying traffic due to enter Center control (but note the huge area NY ARTCC covers). I am not aware that such a circumstance has ever occurred, but given the projected growth in commercial air traffic, it is something to worry about for the future.

Computers and ATC were discussed in [RISKS-17.17](#) (James), 17.18 (Wolper), 17.21 (Burststein, Schultz), 17.24 (PGN), 17.25 (Runes, Karagianis, Ladkin, Pettit), 17.26 (PGN, Margolin, Zellweger), 17.27 (Gelato), 17.28 (PGN), 17.35 (Lucero), 17.36 (Tignanelli, 2 articles), 17.38 (Ladkin), 17.40 (PGN, Ladkin), 17.41 (Tignanelli, Emerson), 17.44 (Goldstein, see also Harding, Menon), 17.49 (PGN), 17.50 (PGN), 17.62 (Kabay), 17.70 (Wolper). It seems as if 1995 was a good vintage ... [Especially if you don't wine too much. PGN]

ATC Communications were discussed in 17.44 (Harding, Menon), 17.64 (Lucero), 17.65 (Ladkin).

Peter Ladkin

US Charges Man Planned to Kill 4,000 Travelers (Reuter)

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

Fri, 31 May 96 15:46:42 PDT

Reuter reported on 29 May 1996 that U.S. prosecutors accuse Islamic militant Ramzi Ahmed Yousef (a.k.a. Abdul-Basit Balochi) and two others of plotting to bomb 12 U.S. jet planes in two days during 1995. Some of the evidence is based on a file found in Yousef's laptop computer, stating that the purpose of the bombings was ``vengeance and retribution'' against the United States for its financial, political and military support of Israel. (Yousef will be tried later this year for masterminding the 1993 World Trade Center bombing that killed six and injured more than 1,000 people. He is also accused of placing a bomb on a Philippine Airlines flight from Manila to Tokyo on 11 Dec 1994, which killed one passenger and injured 10 others.)



Ken Knowlton <KCKnowlton@aol.com>

Fri, 31 May 1996 12:00:000001 pm EDT

Responses to my 12 am/pm = noon/midnight? were mostly of these three forms:

1. 12 am is midnight, dummy; don't bother me with this.
2. Either can mean either; don't use these notations.
3. Tuesday goes from "12am Tues" to "midnight Tues" (and

12am = midnight)!

My conclusions:

1. Be careful in making assumptions about other people's assumptions.

2. I bet that somewhere in this world there's a routine that occasionally

time-stamps with the ASCII string "... 12:00 am" and a backup, restore

or merge routine that later misunderstands the date (misidentifying

the most recent version of a file, or whatever).

I think I can demonstrate how easy it is to make risky assumptions about

other people's assumptions, particularly regarding the phenomenon "don't

need this case -- it just couldn't get here." We all know what scalene and

isosceles and equilateral triangles are, likewise we have crisp ideas about

squares, rhombuses, rectangles, parallelograms and trapezoids, yes? I

invite you to demonstrate to yourselves your knowledge of inclusion/intersection/exclusion relations among these objects by filling in

each of the following blanks with a 'No' or 'Some' or 'All'.

Use your own

self-assured knowledge here -- don't use a dictionary or other authority.

Please *don't* send me your answers unless you can fill in all the blanks

exactly as you think every responsible geometrician would.

Assume that all

figures are planar and non-degenerate:

No/Some/All

___ equilateral triangles are isosceles triangles.

___ equilateral triangles are scalene triangles.

___ isosceles triangles are equilateral triangles.

___ isosceles triangles are scalene triangles.

___ scalene triangles are equilateral triangles.

___ scalene triangles are isosceles triangles.
___ squares are rhombuses.
___ squares are rectangles.
___ squares are parallelograms.
___ squares are trapezoids.
___ rhombuses are squares.
___ rhombuses are rectangles.
___ rhombuses are parallelograms.
___ rhombuses are trapezoids.
___ rectangles are squares.
___ rectangles are rhombuses.
___ rectangles are parallelograms.
___ rectangles are trapezoids.
___ parallelograms are squares.
___ parallelograms are rhombuses.
___ parallelograms are rectangles.
___ parallelograms are trapezoids.
___ trapezoids are squares.
___ trapezoids are rhombuses.
___ trapezoids are rectangles.
___ trapezoids are parallelograms.

Ken Knowlton

[... and Ken is NOT a square. While at Bell Labs in the
1960s, his
programming language BEFLIX pioneered computerized animation;
he also
did L6, among other things. PGN]

⚡ re: TILT! Counterfeit pachinko cards ... (Wayner, [RISKS-18.15](#))

Chiaki Ishikawa <ishikawa@personal-media.co.jp>
Tue, 28 May 1996 22:09:28 +0900 (JST)

I would like to add some background as someone who has played in
pachinko
parlors in Japan. (The origin of the game of pachinko is rather
vague.

Some say it is based on the ball game popular after the WW-II in U.S.A..

Anyway, it is a gambling business.)

The card in question acts as a kind of debit card inside the pachinko parlors. It was introduced a few years ago by an former police official, with the expressed intention of keeping the money flow easy to track. (I would say it was a ruse to make a few companies where the ex-police officials can find jobs after retirement from the office. But I digress.)

The cards are sold to the pachinko parlors and the customers buy the cards from the parlors, and obtain steel balls to play the game by inserting the card into the slot next to the game machine.

Pachinko gambling works as follows. When you win the game, the number of steel balls in your possession increases and the customer can exchange the balls with gifts. (Therein lies a complication. Japanese law prohibits gambling, and so exchanging the steel balls with real money is illegal.

However, first exchanging the balls with gifts, and then exchanging the gifts with money at a third party outlet [which is quite likely to be operated by the parlor owner] has been allowed by the police.)

Speaking of loophole! Some people do bring back the gifts to homes: depending on the places, parlors carry game-boy cartridges, latest bestseller books, snack food such as cookies, instant noodles, umbrella, purse, movie video tape, music CD, to name a few as gifts. But if the customer wants to exchange

his/her win indirectly to money at the outlet, then he/she has to ask for special gifts used essentially as money tokens by these establishments. These are often a tiny gold/silver foil embedded in thin plastic slab, etc.. Each parlor/outlet pair uses different stuff. In my hometown, a special brand of silk stocking was used as money token. This whole thing is a farce in view of the anti-gambling law in Japan.)

Back to the card: the cards in question are used by two leading card manufacturers. (There are another couple of late-entry companies whose cards are not known to be attacked yet.) The card is based on the design done by NTT Data. NTT is the Japanese equivalent of old Ma Bell in the USA. NTT Data is a company that specializes in computer software integration, communication and such. I believe it designs the telephone card (debit card used for pay-phone in Japan), too.

The pachinko card is the size of name card and plastic. The details are not published. To the best of my knowledge, I think there is a magnetic strip that contains the card ID information such as its serial number and the amount of debit money.

There were 10,000 yen, 5,000 yen, 3,000 yen, 2,000 yen, and 1,000 yen cards. (I said "were" because 10,000 yen and 5,000 yen cards are no longer available.)

Attack method:

>From what I saw and read, the first card verification mechanism

used by the pachinko game machine was so primitive to defy rational explanation: each time the card was used, a tiny hole was punched to indicate the amount left in the card. As the customer uses the card, the position of the punched hole on card shifts toward the zero position. Once there is a hole on the zero position, the card is no longer usable.

The first simple attack as far as I can tell was to fill in the hole in the card with tiny plastic (essentially the chaff produced when the hole is punched was used to fill in the hole). I am not sure if such simple attack was possible, but it seemed possible really at the beginning with crude modification of the magnetic data.

Then, of course, the magnetic information on the card was also modified in more sophisticated ways when the card was used.

However, the bad people also learned and somebody stole the reader mechanism and figure out the part of the magnetically-coded information: the result was that bad people could buy the pristine 10,000 yen card and then uses up to 2500 yen of the debit amount legally and then "re-fill" the card to 9500 yen worth, thus gaining 2000 yen for free again and again. (Until 3000 yen was used from the 10,000 yen card, the physical hole was not produced on the card, and only the magnetic information was changed. Hence the mere counterfeiting of the magnetic information was necessary to "revive" the card. No physical re-filling of the card was necessary. Physically

re-filling the hole is easy to spot visually and was avoided by the bad guys.)

[I have to confess that the exact amount involved in the counterfeiting is a little uncertain. But the general idea still holds.]

Similar attack was possible with 5,000 yen card.

Presumably the gain by attacking 3,000 yen, 2,000 yen and 1,000 yen card was small compared with the risk, the bad guys didn't attack these cards until lately.

Now the situation is that of cats and mouse. New counterfeiting methods and counter-measures follow each other in rapid succession.

I believe that the cloning of the card was also done. But I don't know the details.

Now, the card companies and pachinko parlors stopped issuing 10,000 yen and 5,000 yen cards because the damage was so large.

Also, they have installed special readers to verify the validity of the card by incorporating more vigorous checking not available on the readers next to the game machine: it used to be that the cards sold could be used by any pachinko parlors in Japan. Now cards sold elsewhere have to be verified with this machine before used at a local game parlor. Cards sold at the local parlor can be used without such checking.

Already, there are reports of counterfeit-card usage:

- either the cards are so sophisticated that they can pass the

enhanced

reader.

- Or the bad guys buy the cards locally and then use some of the debit amount and then bring the cards to their factory to re-fill and re-use it at the local store again and again.

The card companies have installed countermeasures in selected stores to the cloning of the card by checking the serial number of the card and stopped the operation of the whole game machines in the store if a card with the serial number of the previously used (finished?) card is ever inserted into the game machine.

Another simple method of fooling the reader was also reported about a month ago. Essentially, it cuts out a long strip of the 3,000 yen card (now the most expensive card after 10,000 yen and 5,000 yen card are gone) and rotates the strip to invert its direction and then reassembles the card again using cement or something. To my surprise, it was reported to be deemed valid by some readers (!?). Apparently some readers only check for the position of the hole on fixed position and fooled to believe the card is valid if the hole is not in the expected position, etc.. Once not so rigorous readers are distributed, it is very difficult to upgrade all of them in Japan, I guess.

The problem is complicated in that the counterfeiting only damages the card company. The parlors report the amount of debit money used in their shops and then compensated for the amount (less the small surcharge by the card

company.) This means that every time the counterfeit card is used the card company alone loses money and the local parlor doesn't lose.

There have already been reports of the owners of the pachinko parlors involved in the usage of the counterfeit cards. These bad owners allowed the bad guys to use the counterfeit cards in their parlors and pass the used debit amount to the card company and getting compensated.

In these cases, the bad guys bring back the money (by simply exchanging the phony debit money into the steel balls, and then without playing (they can play if they wish), exchange the steel balls to the special gifts, and then exchange the gifts with money. [Usually, buying the steel balls and then exchanging them with gifts, and subsequently with money leaves you less money than you started with. The house always wins. In this case, the bad guys started out with counterfeit debit money and ends up with real money, so it is OK for the bad guys.] The parlor also gets the money for the used debit money. So they win, too. Only the card companies lose.

Counterfeiting probably has existed since the first money (or equivalent) was ever invented. But, it surprised me that NTT Data approached the whole scheme so naively, especially since there have been reports of telephone card counterfeiting in Japan before. Some of the counterfeiting methods reported seemed so simple, and I have a doubt whether NTT Data was serious enough to deter counterfeiting.

At least, I can safely say they have underestimated the

ingenuity of the
counterfeiters badly and didn't learn from the counterfeiting of
telephone
cards very well.

Ishikawa, Chiaki (family name, given name)
Personal Media Corp., Shinagawa, Tokyo, Japan 142
ishikawa@personal-media.co.jp

🔥 Timing out e-mail -- "kidsciencenet" spam

Laurence Brothers <quasar@bellcore.com>

Wed, 29 May 1996 11:18:38 -0400

I recently received the following (names deleted to protect the
possibly
innocent):

> Subject: kidsciencenet

>

> Hi, our names are XXXXX and XXXXX. We are in the 5th grade at
the

> XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX, Massachusetts, USA. We are

> doing a science project on the Internet. We want to see how
many

> responses we can get back in two weeks. (We are only sending
out 2

> letters).

>

> Please respond and then send this letter to anyone you
communicate

> with on the Internet. Respond to XXX@tiac.net.

>

> 1. Where do you live (state and country)?

> 2. From whom did you get this letter?

>

>

>

Thank you,

XXXXXXXXXXXXXXXXXXXX

I did NOT delete any original mail headers; the only headers

were those of some intermediate remailers who had forwarded only the contents of the "original" note.

God help the ISP for tiac.net if this thing spreads as much as it seems likely to do. I read this on a msgs board with hundreds of other readers, which was only one of the many destination recipients of the intermediate link in the chain who remailed this.

First of all, let's assume this is an honest, innocent post, not a hoax of some sort. Let's note to begin with that as indicated by the mail cc's and headers, those "2 letters" which were sent out have already been multiplied a hundredfold across the internet by people who thought it was a cute idea.

Let's note further, to our horror, that there is no date on the note indicating even when the "two weeks" is up. I'm very much afraid that this may go on for decades (if it hasn't already :-0).

In fact, by asking around, I've found that at least one posting of this note was sent out more than two weeks before the one I saw and copied here.

The general risks of the deliberate exploitation of wide e-mail distribution are obvious and have been discussed many times, but more specifically we can see a problem with an intended timed mailing for which the expiration date was either lost, modified, or never provided in the first place (as in this case).

Laurence R. Brothers ~ quasar@bellcore.com

✉ Access to psychiatric records

<Bob_Frankston@frankston.com>

Sat, 18 May 1996 14:11 -0400

There is an article in **The Boston Globe** 18 May 1996 entitled "AG to probe access to psychiatric records". As usual, one has to guess what is really going on and who is confused about what.

Apparently a local HMO has been including psychiatric records in its medical history database. The first problem cited was the lack of effective access control on that portion of the records. The HMO claims to have "..installed software that limits access to the detailed notes ...".

The other problem is that, apparently, by placing the psychiatric history in the medical record it becomes available to insurance agencies once the patient has signed a release.

This seems to be a typical case of the computer forcing an issue that was already lurking. Medical records are medical records. It seems that it was an implicit (or even explicit) artifact of the paper system that the access was controlled and, perhaps, the insurance companies did not get access. And this was probably a good policy. But it might not have been legal if the insurance companies have access to all records.

As an aside, I think that under Massachusetts law that patient has access to all records which would presumably including the psychiatric

transcripts. And records mean any scribbles. Am I wrong on this?

Is this a matter of an issue being forced by the computerization? Does that mean we must go back to shoeboxes so that records can be "lost" in order to protect privacy?

✶ Smartcards and medical data standards

Peter Bray <"pabcse@airmail.net"@server.airmail.net>
Sun, 19 May 1996 10:21:42 -0700

There is a risk that the rapid and competitive evolution of Smart Card technology will result in a proliferation of data format standards that are proprietary or national in nature. In particular, information categories peripheral to financial transactions could suffer and the potential benefits go unrealized in the immediate term. Medical data, particularly physician to physician alerts and prescription medications and administration regimes are an example. What principles should govern the programme to develop such standards?: Keep it simple and extensible and end-use focused. Aim to keep it international and spoken language independent. Build in configuration management and downward compatibility as medicine and the delivery technology evolve. Include communication protocols for further information. Do not neglect promotion and training plans for practitioner's.

Peter Bray pabcse@airmail.net

⚡ Re: Largest Computer Error in US Banking History? ([RISKS-18.14](#))

"Louis Koziarz" <koziarz@mcs.com>

Wed, 22 May 1996 22:12:31 -0500 (CDT)

(From talking with a knowledgeable friend in the banking/ATM business:) The First National Bank of Chicago/Cash Station 'glitch' was apparently the result of a programming change intended to support the new out-of-area ATM fees being proposed by various banking groups. When the new transaction messages were introduced to the network, some systems took the strange new codes and transformed them into something they could understand: a posting of a huge credit to one's account.

The RISKS here may be more serious than the traditional glitches in electronic financial transactions. What should transaction-based systems do with unrecognizable or foreign input?

⚡ Risks of Statistics in [RISKS-18.13](#)

Frank Fay <f.fay@ieee.org>

Thu, 23 May 1996 12:06:01 -0700

Part 1 (Computer as Goat): Post-divorce wage gap statistic turns out to be computer error

This is a rather old story and computer errors are the least of the problems here. Readers wishing a fuller well-documented account should see Susan Faludi's book "Backlash" (1991), 1st edition, pages 19-25.

According to this account, Weitzman's book "The Divorce Revolution" was published in 1985, contains the -73%:42% figures (for reduction and increase in income after the 1st year of divorce), which are from a small sample size (114 men; 114 women) of interviews from a low response rate of the divorcing population in Los Angeles County. The financial information is based on the memory of those interviewed! As early as 1986 the findings were questioned by other divorce researchers whose own data indicated figures of -30%:10%-15% (close to the recent -27%:10% figures for re-analysis of Weitzman's data). Requests for Weitzman's data, for re-analysis, remained unfulfilled until late 1990 after appeals to the National Science Foundation.

According to the 1996 AP article Weitzman still cannot identify the source of the error ("She blames the loss of her original computer data file, a weighting error or a mistake in the computer calculations performed by a Stanford University research assistant."), and has left the re-analysis of her data to other researchers (Richard Peterson in this case).

As Faludi's extensively-documented book points out the conclusions of poorly conducted studies have real political and legal consequences. In addition they make "social science" more of an oxymoron, and hinder the efforts of those researchers who do good, repeatable work in these fields.

Part 2: Internet in danger (Nazi hate literature)

Jim Carroll seems to be misinterpreting the 80% statistic in several ways:

First, hate literature is likely a small fraction of all literature.
Therefore 80% of a small number is an even smaller number.

Second, he should find out "what 80% means?". I have seen this figure in the past, and I believe the context is regarding published Nazi hate literature available by mail in Germany. I am not sure that the figure even includes e-mail or the Internet at all.

Third, the 80% of hate literature originating from Canada statistic does not imply "80% of Canadians" at all. Canada as a free-speech nation happens to be a convenient safe point from which to send this stuff. Furthermore this probably does not imply that the literature was written or published in Canada. I would suspect that a good deal of it comes from my country, the United States.

[See a recent Sunday New York Times Magazine cover article for more background.]

Frank Fay f.fay@ieee.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 18: Issue 17

Tuesday 4 June 1996

Contents

- [MARTA train jumps track](#)
[Stephen Cohoon](#)
- [Taipei subway computer crash](#)
[Calton](#)
- [New book by Peter Wayner on crypto and steganography \(hide and seek\)](#)
[PGN](#)
- [Report Opposes Administration's Cryptography Plans](#)
[Edupage](#)
- [New form of harassment; third-party paging](#)
[Joe Smith](#)
- [Cyber-terrorists blackmail banks and financial institutions](#)
[The Dodger](#)
- ["Secret lie-detector test from a distance"](#)
[Daniel P. B. Smith](#)
- [MIME bites equations](#)
[Geoff Kuenning](#)
- [Loopy Mail](#)
[Kevin Rainier](#)
- [Risks of insufficient concept design](#)
[Andrew Pam](#)

- [Election "Glitch" in Capetown](#)
[David Kennedy](#)
 - [Roundoff error on Detroit Edison bills](#)
[Jim Rees](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✈ MARTA train jumps track

Stephen Cohoon <cohoon@snt.bellsouth.com>

Mon, 3 Jun 1996 11:02:23 -0400 (EDT)

On Saturday, June 1, 1996, a commuter train operated by the Metro Atlanta Regional Transit Authority (MARTA) had one car leave the track causing injuries to 19 people and much embarrassment for the "Official Spectator Transportation System" for the Olympic games.

According to local TV news and newspaper reports, the train had stopped before a red signal apparently on automatic control. The operator called dispatch requesting permission to go to manual. Permission was granted and the operator proceeded *through the red signal* setting off alarms. The train was stopped and put into reverse. As one of the middle cars passed over a crossover switch some or all of its wheels were lifted and displaced. The train stopped very suddenly tossing the operator and 18 passengers from their seats. MARTA does not consider this a derailment because no cars fell on their sides.

A MARTA person interviewed on camera said there is no time that any train on manual or automatic should pass a red signal. The operator, the

supervisor

on duty and the dispatcher have been suspended pending a review.

Personal opinion: this is a familiar scenario often repeated in RISKS but

apparently not yet learned by those responsible for critical safety systems.

Operator training and supervision must exceed the the capacity of a system

to cause harm to people. Manual overrides must be designed to increase

safety not allow safety systems to be subverted. In 47 days over a million

people will come to Atlanta. There is no way MARTA can repair the public

relations damage caused by this incident in that time.

I ride the line on which this happened every day. In the 4 years I have

been here I have found MARTA to be a safe and reliable system compared to

the alternative of driving through the daily carnage of the freeways. I

will continue to use MARTA even though this incident has been a disappointment to me. Perhaps this will cause heightened vigilance and

improved supervision which may help prevent a larger disaster while every

news reporting organization in the world is in town.

Stephen M. Cohoon BellSouth Telecommunications 675 W. Peachtree St. NE

Room 41G70 Atlanta, GA 30375 cohoon@snt.bellsouth.com (404) 332-2275

[You wouldn't want to be a MARTA to the cause-way! PGN]

Taipei subway computer crash

<calton@cse.ogi.edu>

Tue, 4 Jun 1996 19:13:28 -0700

Taipei's only subway line service was completely disrupted on Monday morning, 3 June 1996, due to the simultaneous shutdown of both the main computer and the backup system. The control center ordered an emergency shutdown of the entire system, which did not cause any train accidents or casualties.

The subway company reported that at 9:27am on that morning, the main control computer suddenly printed out 14 pages of extraneous program code. Eight minutes later, both the main control computer and the backup system went down. Maintenance engineers, with the help of a Matra engineer (the company that supplied the control software), were unable to reboot either system. Digital engineers (the company that supplied the hardware) arrived shortly and discovered that one of the rebooting programs was missing. They reloaded the rebooting program from backup media and the subway line/system returned to normal functions after four hours and thirty-four minutes.

The situation is complicated by the recent breakdown in contract negotiations between the subway company and Matra for maintenance. Matra has taken back most of its maintenance personnel, but the subway company has not fully acquired the capability for maintaining the entire system, including the computing system, particularly the proprietary control software written by Matra.

The subway company presumes the incident to be sabotage and has

asked the police authorities to investigate. The police computer experts have declared that it is difficult to investigate the control software consisting of more than ten millions lines of code. Furthermore, the police have not ruled out the other possibilities such as operator error and software design error.

In the public opinion section of the same newspaper, several readers discussed the risks involved in this kind of incident. The section title was "The important question is: who should be responsible for computer security", subtitle "who sabotaged the computer is secondary."

(Source: digest/translation of news from United Daily News, Taipei, 5 June 1996.)

[5 June? Oh, yes, remember the International Date Line. But if you indulge in international dates in Taipei, be prepared for Matra-mony. And note that MARTA and Matra are anagrams. They seemed to belong together. PGN]

🔥 New book by Peter Wayner on crypto and steganography (hide and seek)

"Peter G. Neumann" <neumann@csl.sri.com>
Mon, 3 Jun 96 16:42:10 PDT

Cryptography is certainly not the only way to hide information, and in some

cases perhaps not even the best way. For a delightful easy-to-read book on a range of related topics with particular attention to steganography (for example, hiding information so that it perfectly naturally looks like something else, such as making your encrypted PGP message look like a .gif file of the Mona Lisa), consider Peter Wayner's new book. It is a gold mine full of fascinating nuggets, and they all seem to fit together into a brand-new golden oldie.

Peter Wayner, *Disappearing Cryptography: Being and Nothingness on the Net*,

AP Professional (Academic Press), Chestnut Hill, Massachusetts, 1996.

Report Opposes Administration's Cryptography Plans

Edupage Editors <educom@elanor.oit.unc.edu>

Sun, 2 Jun 1996 15:19:35 -0400 (EDT)

Rejecting Clinton Administration arguments that law enforcement efforts would be hampered by cryptography technology now based on a "key escrow" system allowing the government to decode any electronic communications after obtaining a court order, a report prepared for the National Research Council of the National Academy of Sciences says that unbreakable cryptography would actually help prevent crime by preventing criminals from intercepting legitimate business transactions. The report recommends dropping steep export controls currently placed by the government on products using the

56-bit key Data Encryption Standard, which offers significantly greater communications security than the 40-bit-key code that may be freely exported. (*The New York Times*, 31 May 1996, p. C1; Edupage 2 June 1996)

[The executive summary of the report can be found at <http://www2.nas.edu/cstbweb> . PGN]

✈ New form of harassment; third-party paging

Smith and O'Halloran <inwap@best.com>

1 Jun 1996 18:14:36 -0700

Summary: Tricking pager owners to do the harassment for you

While trying to catch some Zs, my pager went off twice in quick succession.

The number was one I did not recognize, XXX-XXXX-911. I called the number

and a limousine service answered. Turns out that some guy had been

harassing the women there over the phone, and now he has gotten innocent

bystanders to help him unwittingly. Apparently this guy obtained a list of

pager numbers (or found an exchange that is densely populated with pager

numbers) and is sending the limousine company's phone number out. The

police are involved, but are having a difficult time tracking down the

culprit. They believe he is using one or more pirated cellular telephones.

Joe

INWAP.COM is Joe and Sally Smith, John and Chris O'Halloran (and

our cats).

✶ Cyber-terrorists blackmail banks and financial institutions

The Dodger <dodger@spodbox.linux.org.uk>

Sun, 2 Jun 1996 14:52:03 +0100 (BST)

The following article appeared on the front page of the
Sunday Times

(a British newspaper) on Sunday, 2 June 1996, under the banner
headline 'City surrenders to 400m-pound gangs':

City of London financial institutions have paid huge sums to
international
gangs of sophisticated "cyber terrorists" who have amassed up to
£400m
worldwide by threatening to wipe out computer systems. Banks,
broking firms
and investment houses in America have also secretly paid ransoms
to prevent
costly computer meltdown and a collapse in confidence among
their customers,
according to sources in Whitehall and Washington.

An Insight investigation has established that British and
American agencies
are examining more than 40 "attacks" on financial institutions
in New York,
London and other European banking centres since 1993. Victims
have paid up
to £13m a time after the blackmailers demonstrated their ability
to bring
trading to a halt using advanced "information warfare"
techniques learnt
from the military.

According to the American National Security Agency (NSA), they
have
penetrated computer systems using "logic bombs" (coded devices
that can be

remotely detonated) electromagnetic pulses and "high emission radio frequency guns", which blow a devastating electronic "wind" through a computer system. They have also left encrypted threats at the highest security levels, reading: "Now do you believe we can destroy your computers?"

The authorities have been unable to stem the attacks, which are thought to originate from the United States. In most cases, victim banks have failed to notify the police. "They have given in to blackmail rather than risk a collapse in confidence in their security systems," said a security director at one blue-chip merchant bank in the City. A senior detective in the City of London police said: "We are aware of the extortion methods, but the banking community has ways of dealing with it and rarely reports to the police."

European and American police forces have set up special units to tackle the cyber criminals who, Ministry of Defence sources believe, have netted between £200m and £400m globally over the past three years. But law enforcement agencies complain that senior financiers have closed ranks and are hindering inquiries.

Experts in information warfare met in Brussels last month to discuss defensive measures. Representatives included Captain Patrick Tyrrell, assistant director of computer information strategy at the Ministry of Defence; General James McCarthy, professor of national security at the US

Air Force Academy, General Jean Pichot-Duclos, director of the economic intelligence department of the French Defence Council, and senior figures from the civilian computer industries.

A separate closed meeting involving representatives from Whitehall and the intelligence community was held to analyse the 40 attacks on British and American financial centres since 1993. A further secret seminar took place in Washington this weekend.

Kroll Associates, the international investigating firm, confirmed last week that it had acted for financial institutions that have been blackmailed.

"One of the problems we face is that the potential embarrassment from loss of face is very serious," said a spokesman in New York. Kroll had evidence that firms in London and New York had been targeted. "The problem for law enforcement is that the crime is carried out globally, but law enforcement stops at the frontier," he said.

Yesterday a Bank of England spokesman acknowledged the threat from extortionists: "We are aware of this. It does exist. It is extortion and fraud." But the spokesman also insisted: "It is not the biggest issue in the banking market."

Scotland Yard is now taking part in a Europe-wide initiative to catch the cyber criminals and has appointed a senior detective from its computer crime unit to take part in an operation codenamed Lathe Gambit. Such is the secrecy that few details about the inquiry have emerged.

In America, the FBI has set up three separate units to investigate computer extortion. The NSA believes there are four cyber gangs and has evidence that at least one is based in Russia. The agency is now examining four examples of blackmail said to have occurred in London:

- o January 6, 1993: Trading halted at a broking house after blackmail threat and computer crash. Ransom of #10m paid to account in Zurich.
- o January 14, 1993: a blue-chip bank paid #12.5m after blackmail threats.
- o January 29, 1993: a broking house paid #10m in ransom after similar threats.
- o March 17, 1995: a defence firm paid #10m in ransom.

In all four incidents, the gangs made threats to senior directors and demonstrated that they had the capacity to crash a computer system. Each victim conceded the blackmailer's demands within hours and transferred the money to off-shore numbered accounts, from which it was removed by the gangs within minutes.

The techniques have varied. In London, criminals posing as marketing firms have gained detailed knowledge of a target's system by interviewing the heads of information technology departments. In some cases, they have even issued questionnaires to unsuspecting officials. Armed with this information, they have been able to breach security and leave encrypted messages warning of their capability.

The gangs are believed to have gained expertise in information

warfare techniques from the American military which is developing "weapons" that can disable or destroy computer hardware. Some are also known to have infiltrated banks simply by placing saboteurs on their payroll as temporary staff.

Little is yet known about the identities of the gangs, but, according to the NSA, America is the main source of the attacks. It believes that at least one other group originates from Russia and has followed the movement of money to the former Soviet States.

A spokesman for the Metropolitan police said: "There is potential for extortion from those purporting to know how to damage computer systems. "The computer crime unit liaises where necessary with it's Euro counterparts to discuss cross-frontier crimes."

One merchant bank director said yesterday: "You will never get a financial institution to admit it has an extortion policy, let alone that it has paid money to blackmailers."

Personally, I view this story with marked scepticism. I have no doubt that it is true to a certain extent, but the idea of banks forking out ten million pounds (circa \$14m) to a blackmailer is one I find slightly unrealistic.

In any case, I'm sure we'll hear more about this story in the future.

The Dodger
dodger@spodbox.linux.org.uk

<http://spodbox.linux.org.uk/~dodger/>

⚡ "Secret lie-detector test from a distance"

"Daniel P. B. Smith" <dpbsmith@world.std.com>

Tue, 4 Jun 1996 11:01:12 -0400 (EDT)

Computerworld, 3 June 1996, p. 4, "Patent Watch" says that patent 5,507,291 covers "a system for remote analysis of a person's emotional or metabolic state, such as performing a secret lie-detector test from a distance. Energy waves are reflected off the object to determine blood pressure, pulse rate, pupil size, respiration rate, and perspiration level. A computer compares the readings with normal levels."

And HAL could only read lips!

Daniel P. B. Smith dpbsmith@world.std.com

⚡ MIME bites equations

Geoff Kuenning <geoff@ficus.cs.ucla.edu>

Wed, 29 May 1996 12:57:36 -0700

A few days ago, a subscriber to Yacht-L (a sailing-related mailing list) decided to post a few useful equations to the list. Some of the equations involved time/speed/distance conversions, with distance represented by "D".

Unfortunately, he used a MIME-enabled mailer to do the posting,

and
MIME decided that the nasty old "equals" sign was a sufficiently
weird
character that had best be encoded in hex. It happens that the
proper
hex is "3d", but MIME likes upper-case -- and to make matters
really
bad, it introduces the hex code with an equals sign.

So the equation:

$$S = D / T$$

became:

$$S = 3D D / T$$

to the great confusion of many list subscribers, who couldn't
understand why you would want to square and triple the distance
in
such a simple equation.

The RISK? When inventing a standard, one should consider the
impact
on non-conforming systems.

Geoff Kuenning g.kuenning@ieee.org geoff@ITcorp.com
<http://ficus-www.cs.ucla.edu/ficus-members/geoff/>

[We have been around this basic problem before in RISKS on
several
occasions, but the problem keeps biting me in attempting to
moderate RISKS, so I am not surprised to find new instances.
PGN]

Loopy Mail

Kevin Rainier <Kevin_Rainier.NOTES@crd.lotus.com>
4 Jun 96 14:20:39 EDT

It all started innocently enough. Last night somebody sent a message to the recreational mailing list "virtua-fighter@netcom.com". This is an infrequently used mailing list for the discussion of the Virtua Fighter family of SEGA arcade games. Since the last time somebody had used the list a Microsoft employee left the company -- perhaps he died -- and the mail address is no longer valid. Microsoft is a helpful company and informed the list (automatically, of course) that the address is not valid. Netcom is a helpful list server and sent the message to all recipients of the list, including the late, lamented employee of Microsoft. And so it continued. And continued.

It's now morning. I'm receiving a message every two or so minutes, the subject line has maxed out with "Undeliverable: Undeliverable: ...". Members of the list have just begun arriving at their desks and discovering over 150 messages from postmaster@microsoft.com via the virtua-fighter mailing list. Naturally, they panic and rush to unsubscribe from the list. Not knowing how to do that, they send an "unsubscribe" message to -- where else -- "virtua-fighter@netcom.com". Which sends a message to the user at Microsoft. So far we've had five attempts to unsubscribe.

As I've been composing this mail, the frequency of new mail has increased to more than one message per minute.

Oh no. There's a bad address at dartmouth.edu. It replied to the list too. I suppose I can hope that it won't reply to its own replies.

But I'm sure that Microsoft will. And since the Dartmouth message is responding to a Microsoft "Failed Mail" message, that part of the loop is working just fine.

Hmm, I just found out that our outgoing mail server isn't working, though our incoming one is working just fine.

I love computers.

One final postscript: I just received a message (two hours after the above portions were written) from the list maintainer -- the list is now dead. I also haven't received any new autoreply messages for an hour. Seems that the storm has passed.

kevin_rainier@crd.lotus.com

[If the RISKS experience is any indication, there are days on which

I get 20 or 30 NEW bounces on addresses that worked the day before.

One new bounce an hour would have added more to your enjoyment. PGN]

⚡ Risks of insufficient concept design

Andrew Pam <avatar@glasswings.com.au>

Mon, 3 Jun 1996 23:37:12 +1000 (EST)

I've just seen the announcement for a new Web server facility called SiteShield(tm) (see <http://maximized.com/products/siteshield/>)
>From their marketing information:

: SiteShield is an exciting new concept in Web content protection.
: SiteShield permits content providers to place copyright-protected images
: on web pages without the fear that they can easily be stolen and
: re-used. Employing proprietary server-based technology, SiteShield
: allows webmasters to simply indicate which images need protection.
: Finally, webmasters can feel confident that the images they are placing
: on web sites are being protected.

What it appears to do is send an intentionally corrupted image if the
Referer: header indicates that the page from which the image was referenced is not on the same site as the image itself.

There are a number of problems with this concept, but the most glaring
is that once the image has been displayed on the screen it can easily
be captured and saved to a file, thus completely defeating the entire
purpose of the product.

The Xanadu solution is to transcopyright the images, granting prior
permission for them to be referenced online providing a link back to
the original site is maintained.

THE RISKS? Well, apart from the obvious risk that the product may
well fail since it can be so easily defeated, it probably also won't
work with older browsers that don't return the Referer: header and
is known to have problems (as you would expect) with caches.

Andrew Pam, Coordinator, Xanadu Australia, Technical Editor,
Glass Wings,

Manager, Serious Cybernetics xanni@aus.xanadu.com +61 3
96511511

⚡ Election "Glitch" in Cape Town

David Kennedy <76702.3557@CompuServe.COM>
03 Jun 96 18:08:45 EDT

Courtesy of Reuters News via CompuServe's Executive News Service:

Counting glitch delays final Cape Town result

Reuters Financial Report 6/1/96 10:34 AM

>> CAPE TOWN, June 1 (Reuter) - A computer error forced
>>officials on Saturday to award South Africa's ANC an extra seat
>>in Cape Town's first post-apartheid city election and the
>>glitch will delay the final outcome until next week.

>> Election officials said 2,000 ANC votes and one seat in the
>>city's Tygerberg area, which includes the black township
>>Khayelitsha where the party is strong, had wrongly been given
>>to a tiny religious party. [...]

>> Results were expected on Friday or shortly thereafter but
>>the formula under which the council is elected -- a mix of ward
>>seats and proportional representation -- will now have to be
>>put through computers again. [...]

[DMK: To see if the glitch is reproducible? The article is
chiefly about SA
politics, with no specific description of the "glitch" and
actions to
prevent it from reproducing.]

>> ANC officials said they wanted a swift explanation from the
>>chief election officer about what went wrong and would consider
>>court action over the election results if he failed to respond.

>> "If they could make that mistake in one ward, the chances
>>are that other mistakes have been made elsewhere," Western Cape
>>ANC leader Chris Nissen told Reuters.

Dave Kennedy [CISSP] Information Security Analyst, National
Computer Security
Assoc.

⚡ Roundoff error on Detroit Edison bills

Jim Rees <rees@umich.edu>
Fri, 17 May 1996 19:10:52 -0400

Detroit Edison's residential electric bill has a section titled "Energy Use Report." This section reports incorrect numbers due to improper integer roundoff.

One of the fields gives the average daily energy use for the month in Kilowatt-hours, rounded to the nearest integer value. Another field gives the percent change against the same month for the previous year.

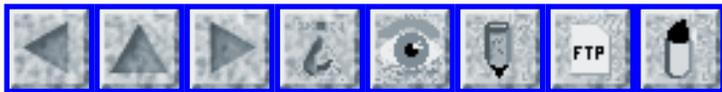
The percent change is calculated using the rounded value for energy use. This can result in large errors. For example, my February 1996 use was 11.68 KWh/day, compared to 11.21 the previous year. After rounding this becomes 12 compared to 11, and the change is reported on the bill as 9 percent ($12/11 - 1$) instead of the correct 4 percent ($11.68/11.21 - 1$).

I wrote to Detroit Edison about this. Their only response was an offer to "assist [you] in understanding how the percentage ... is calculated." Since I already know how it is calculated (incorrectly), I declined the offer.

One RISK would be to assume that the entire bill is correct just because part of it (the billed amount) is subject to government regulation.



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 18: Issue 18

Thursday 6 June 1996

Contents

- [L-vis Lives in Virtual TV](#)
[PGN](#)
- [Another Java attack](#)
[David Hopwood](#)
[Marianne Mueller](#)
- [FORTRAN and heat exchangers](#)
[Thomas Koenig](#)
- [Ariane 5 failure](#)
[Ralphe Neill](#)
[John Rushby](#)
[David Wood](#)
- [Ariane Explosion - Positive Aspects](#)
[Richard Butlin](#)
- [RAL loses satellite cluster to Ariane Five](#)
[Philip Overy](#)
- [Accidental shooting down of F-15 revisited](#)
[Chiaki Ishikawa](#)
- [College Paper Sued Over Quote](#)
[Paul W. Wisneskey](#)
- [Pornography and throughput?](#)
[Andrew Koenig](#)

- [Re: Cyber-terrorists blackmail banks and financial institutions \[Identity withheld by request\]](#)
 - [Fourth ACM Conference on Computer and Communications Security](#)
[M.K. Reiter](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ L-vis Lives in Virtual TV

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

Thu, 6 Jun 96 8:06:25 PDT

L-Vis (Live Video Insertion System) allows arbitrary images to be superimposed on television pictures (for example, for advertising purposes)

but without those images appearing to live audiences or on instant replays.

The Princeton Video Image system "uses missile guidance technology and a customized computer" to insert electronic billboards in the viewer-perceived

program. The computer system recognizes familiar patterns (such as the wall

behind home plate in a baseball stadium) and automagically inserts the

desired logo or other graphic in the specified location. The image is

logically removed whenever it would in the real world be physically obscured

from camera view (e.g., by a batter or umpire). [Source: *San Francisco

Chronicle*, 6 Jun 1996, p. A1 and A13.]

Subliminal advertising was tried in movies back in the 1950s.

This is

perhaps more insidious, because you can no longer tell what is real and what

is virtual. Added icons of virtual victuals depicting the sponsor's

products all over the ball park -- perhaps even on the pitched balls, with

adjustments for spin? The label on the Cincinnati Reds' owner's

favorite

beverage transformed into the sponsor's label, or Schottzie
overlayed as a

pit bull? Think how the TV producers could alter Chicago Bulls'
Dennis

Rodman's appearance (pet bull?), dynamically color coordinating
to adapt to

the arena surroundings. Signs visible to the live audience
(such as "Smoke

El Hempos") could be transformed appropriately (e.g., "DON'T
Smoke El

Hempos") for the TV audience, to satisfy an emerging FCC
broadcast

regulation against tobacco. L-vis has absolutely glorious RISKS-
related

possibilities, such as when the pattern recognizer indentifies
something

that unexpectedly happens to match the given rules. A
contradictory message

might get added to the sponsor's message, or an obscenity might
emerge as an

inadvertent juxtaposition of symbols. Stay tuned for more
excitement

appearing in RISKS on this one! PGN

⚡ Another Java attack

David Hopwood <david.hopwood@lady-margaret-hall.oxford.ac.uk>

Sun, 2 Jun 1996 07:46:20 +0000 (BST)

There is another serious security bug in the class loading code
for all

currently available Java browsers:

Netscape up to versions 2.02 and 3.0beta4 (except Windows 3.
x)

Oracle PowerBrowser for Win32

HotJava 1.0beta

'appletviewer' from the Java Development Kit up to version

1.0.2

Sun, Netscape, and Oracle have been sent details of the problem (which is partly related to the ClassLoader attack found by Drew Dean, et al. in March). The attack works by exploiting a design flaw in the mechanism that separates JVM classes into different namespaces.

Using this bug, an attacker can bypass all of Java's security restrictions.

This includes reading and writing files, and executing native code on the client with the same permissions as the user of the browser.

The only way to avoid this problem at the moment is to disable Java. For more details see

<http://ferret.lmh.ox.ac.uk/~david/java/bugs/>

Technical details will be posted when Sun, Netscape, and Oracle release patches.

David Hopwood david.hopwood@lmh.ox.ac.uk <http://ferret.lmh.ox.ac.uk/~david/>

Another Java attack

Marianne Mueller <mrm@doppio.Eng.Sun.COM>
Thu, 6 Jun 1996 14:15:46 -0700

David Hopwood, a Java researcher in the UK, has uncovered a new security bug in Java [[RISKS-18.18](#)]. In simple terms, he has been able to manipulate the way objects are assigned and the way they collaborate, in order to undermine

the applet security manager.

Hopwood contacted JavaSoft directly re: the bug, and we have had a team working on a fix for the past 72 hours. In addition, we are applying Hopwood's model to conduct a security review, to determine if there are other bugs that may apply.

We are currently thoroughly testing the fix, and plan to release a patch as soon as possible. As we complete more testing of the fix, a more detailed description of the bug and the fix will be added to the JavaSoft security FAQ at <http://java.sun.com/sfaq/>.

JavaSoft is grateful for the internet security community's active interest in reviewing our code and we welcome feedback that makes Java better technology.

✶ FORTRAN and heat exchangers

Thomas Koenig <ig25@fg70.rz.uni-karlsruhe.de>
5 Jun 1996 10:55:06 +0200

This is an old hat, but it still keeps coming up.

A co - worker of mine was doing experiments on a heat exchanger; he was also modelling it with a FORTRAN (77) program that ran on a PC.

One dimensionless quantity used in heat-exchanger theory is the Nusselt number, defined as

$$\text{Nu} = \alpha * l / \lambda$$

(alpha is the heat transfer coefficient, l a characteristic length, and lambda the thermal conductivity).

The name of the variable he chose was NU; he did not declare this variable, so the FORTRAN compiler implicitly typed it as an integer. Since the range of NU was between 10 and 200, this introduced a maximum error of 10% to 0.5% in his calculations - small enough not to be noticed immediately. I don't want to make a bet on how many commercial heat-exchanger design codes make the same error.

Related is the "5/9" problem (this expression silently evaluates to 0 in FORTRAN and C), which often bugs translations of formulas by hand into FORTRAN, which makes $a^{*(5/9)}$ equal to 1.

Some tools (notably ftnchek for FORTRAN 77) recognize this, and issue a warning. Unfortunately, these tools are not in wide use in the scientific community.

[NUsseltoV! PGN]

✶ Ariane 5 failure

Ralphe Neill <ran@rdt.monash.edu.au>

Thu, 6 Jun 1996 20:28:52 +0000

>From the "Electronic Telegraph" (UK Daily Telegraph) - June 6, 1996

"A COMPUTER error swivelled the nozzles of Ariane 5's two giant boosters, sending Europe's most powerful rocket off

course to its destruction, the European Space Agency said yesterday. [...]

"Investigators do not have to collect debris or hunt for a black box. Final analysis of what confused the guidance system will come from a study of the tapes that contain the telemetry messages that constantly reported the status of the launcher's computer and on-board systems. The data will be fed into computer simulators, run by Aerospatiale and CNES, the French space agency."

Given Aerospatiale's record with the Airbus, it'll be interesting to see if they come up with "pilot error" as the cause! :-))

[Also commented on by "Otto J. Makela" <otto@cc.jyu.fi> and Paul Ferguson <pferguso@cisco.com>. PGN.]

✶ Ariane 5 failure

John Rushby <RUSHBY@csl.sri.com>
Wed 5 Jun 96 14:54:47-PDT

>From cnn's web page www.cnn.com:

Faulty computer blamed in Ariane rocket failure

Experts studying the moments before the Ariane-5 rocket explosion say faulty computer software may be to blame for the rocket veering off course. Apparently, the rocket was misfed information that made it think it was not following the right path. The rocket then changed direction, causing the upper part to began to break apart.

⚡ The European Space Agency's little problem

David Wood <david@thermoteknix.co.uk>

Thu, 6 Jun 1996 08:46:31 +0100

After the European Space Agency's little problem this week and the reports now filtering out that it was 'a computer error', it sounds more like a sensor fault or a wiring fault. (Apparently, the computer tried to correct for what it thought was a disturbance to its trajectory and then set the thrusters full over - one big disturbance or was it positive feedback).

Anyway, the ground controls hit the 'explode' button.

Why 0 why didn't the payload have a chute. After all it must have had separator blasts. The 'abort and blow up' sequence could have consisted of a 'separate and chute' the payload stage followed by blow up the rest.

Didn't the early Apollo missions do this, or some other satellite launchers.

Is this complacency at work here.

What a risk - millions of (pounds, dollars, whatever - big in anyone's currency) and all that work.

David Wood d.wood@thermoteknix.co.uk postmaster@thermoteknix.co.uk

⚡ Ariane Explosion - Positive Aspects

Butlin Richard <RMBUTLIN@farnboro01.datasci.co.uk>

Wed, 05 Jun 96 15:04:00 PDT

On 4 June 1996 the Ariane 5 prototype European space launcher veered off course and was destroyed by its controllers 40 seconds after blast-off (details from **The Guardian**, UK 5th June 1996). The launcher development had cost UKP5bn (pounds sterling) and the explosion destroyed a UKP500M four-satellite experiment to monitor the sun, and as the headline says..."And It Wasn't Insured".

Leaving consideration of what went wrong until details emerge, it is worth noting aspects that were successful or at least were not as poorly managed as may appear. Firstly, there was no loss of life - the safety precautions for destruction by ground control worked as planned (the TV pictures showed the destruction happened within seconds of the off-course problems becoming visible, suggesting that either data had already indicated problems or that the controllers were remarkably responsive at pressing a pretty expensive button). Secondly, the European Space Agency is in a risk taking business, and the price of risk taking is occasional failure - Ariane 5 is the follow on to existing Ariane rockets that bring the agency's commercial arm UKP666M per year, with a waiting list valued at nearly UKP3.3bn. Thirdly, regarding the financial losses, it is nigh on impossible to obtain insurance for test flights, and the cargo was being flown for free (the scientists responsible for the experiments didn't have the budget for a paying flight, so took the risk of a prototype launch).

It is certain that there will be lessons from the investigation, but it is worth noting that, but for some risk management at the high level, it could have been much worse and that risks were recognised by the participants, even if not adequately protected against.

Richard Butlin Data Sciences UK (rmbutlin@farnboro01.datasci.co.uk)

✶ RAL loses satellite cluster to Ariane Five

Philip Overy <pjo33@mailbox.rl.ac.uk>

Wed, 05 Jun 1996 15:18:43 +0100

Although the uninsured satellite was carried on a free flight with known risks that it wouldn't work right first time, I think we now know that there's no such thing as a free launch.

Personally I think they should bring back Blue Streak.

Actually, as readers of the Airbus thread will know, I have a bias in favour of the European aircraft industry - whether I would travel in a capsule on Ariane Five is another matter, but I remember the quote about what either John Glenn or Alan Shepherd thought about when waiting to launch ("the rocket contains 5 million parts, all made by the lowest bidder" , approximately) so I suppose launch vehicles will inevitably be either unreliable, or Bad Value For Money - so make sure your satellites are all reproducible by CAD/CAM. And perhaps there should be a few more CASE and

automatic testing systems around?.

So for a change the risk is, there might not be enough computerisation?

Although I sign this stating where I work, this is very definitely my personal opinion, not RAL's!!!, however the destruction of the rocket when it went off course and tried to attack French Guiana made the national news here: I don't think my bad publicity will equal what Ariane has had from the press. The satellite design computer was attacked by organised hackers via Sweden a month or so ago - perhaps this was an indication of how the Eastern Bloc intends to prop up its launcher industry?. In any case, it's worth bearing in mind that this sort of "navigation error" could easily creep in if a virus or a hacker gets onto the development computers. Computer security that's worth money isn't only confined to banks.

Phil Overy Rutherford-Appleton Laboratory, UK

⚡ Accidental shooting down of F-15 revisited (Re: [RISKS-17.56](#))

Chiaki Ishikawa <ishikawa@personal-media.co.jp>

Wed, 5 Jun 1996 21:35:29 +0900 (JST)

Some of the readers of RISKS will recall that I reported an accidental shooting down of an F-15 fighter plane by another F-15 during interception training of the Japanese air force last December.

To refresh your memory, what happened was that

- Two F-15 airplanes took place in an interception training.
- One of the planes carried live missiles.

The reason given was that the airplanes were routinely engaged in

REAL interception missions and taking missiles off takes time.

(BAD decision: They ought to have unload the live missiles in the first place.)

- The main fire unit was supposed to be off (by turning off main switch).

- However, somehow, it got turned on. (static electricity problem?)

- Despite the visual cue on the main firing display console, which showed that the main firing system was ON and live, the pilot triggered the firing button, and launched a sidewinder

missile against another F-15.

- The F-15 was hit and destroyed. The pilot escaped by parachute.

The defense agency released its investigation report on the the accident. (I think it was released last week.) Some newspapers had

articles following the release of the report, but they are all sketchy. My conclusion after reading articles is this.

- Yes, indeed, the main firing system was turned on. But, they could

not determine the cause of the malfunction(!).

- The report seemed to imply that the visual cue on the firing console ought to have alerted the pilot that the system was live

and that the pilot should have taken notice and refrained from

triggering the missile.

(I think Japanese pilots have less live missile traing than, say,

U.S., or Israel pilots, and so pilots may have tough time figuring

out what the real operating modes are from complex computer display alone. Well, this is the reason they need training in the

first place anyway, though.)

- (To my disbelief) It was suggested some type of plastic cap be placed on the main trigger during future training missions to prevent pilots from triggering(!?).

Frankly speaking, I was pretty much dismayed at the depth of of the investigation. It didn't really go to the bottom of the malfunction.

The same hardware/software problem might persist in other F-15s in Japan.

(It was not clear whether same type of problems are ever reported before in the U.S.A.. My understanding is that F-15s used in Japan are licensed and manufactured in Japanese factories. But computer firing systems are often brought in as is from U.S.A. as black boxes.)

The last low-tech solution to the prevention of triggering the missile was almost comical.

Some conspiracy theorists could argue that the air force might want to hide some mistakes during the manufacturing of Japanese version of F-15 by shifting blame on the pilot. But I digress..

Now that the Japanese naval boat shot down a U.S. airplane off Hawaii, I am interested how far the investigation of *THIS* accident goes and what way. I hope they nail down the cause this time around.

Chiaki Ishikawa Personal Media Corp. Shinagawa, Tokyo, Japan
142
ishikawa@personal-media.co.jp

College Paper Sued Over Quote

"Paul W. Wisneskey" <pwwisnes@magenta.com>
Wed, 5 Jun 1996 08:01:02 -0400 (EDT)

>From the Roanoke Times (May 15th, 1996 edition):

> A Virginia Tech official failed to see any humor when a student
> newspaper erroneously listed her job title last month as
"Director of
> Butt Licking. Sharon Yeagle was so unamused she filed an
\$850,000
> defamation lawsuit...

> ...[The paper's] editors say the phrase was part of a computer
system
> template never meant to be published.

The newspaper involved is the Collegiate Times, the student run
paper of
Virginia Polytechnic Institute and State University. In an
article on page
A6 of the April 30th edition, the paper ran an article about
seven students
who were accepted into the Governor's Fellows Program. In the
center of the
article was a featured quote from Sharon Yeagle, an assistant to
the vice
president of student affairs.

Unfortunately for the newspaper, the template used for the layout
contained a "humorous" title meant to be replaced. Somehow the
quote and
quotee were filled in but her title was never entered and the
placeholder, "Director of Butt Licking" was published instead.

And this is not the first time this has happened. According to
the
article in the Roanoke Times, in the Oct. 27th issue the phrase
also
appeared. However, that time an accurate quote was attributed
to a false

name and a false title.

The risks? If you're going to have a generic template, make it generic. And if something bad happens once, it's going to happen again so fix it after the first occurrence. Personally, when I'm writing and need to leave something to be completed later I always enter in a string of at least five question marks. It has become second nature for me to search for that string before "committing" my writing. And when I've forgotten, it has resulted in some confusion but fortunately no lawsuits.

Paul Wisneskey pwwisnes@magenta.com <http://magenta.com/~pwwisnes/>

⚡ Pornography and throughput?

Andrew Koenig <ark@research.att.com>
Thu, 6 Jun 1996 09:36:09 +0400

In [RISKS-18.15](#), Bob Morrell takes an assertion (cited from [RISKS-18.13](#)) that a particular ISP would triple its throughput if it accepted alt.binaries and parlays that into a claim that the Internet is mainly about pornography. Occam's Razor suggests a more general explanation: Images contain much more information than text, regardless of content.

Here is an example. I am writing a book. A picture will fill the front cover; a smaller picture will appear on the back cover. The publisher sent me a JPEG file representing the front cover; that file is

252,368 bytes.

The file with the back-cover picture is 54,070 bytes. Total: slightly more than 306,000 bytes.

The entire text of the book (400 pages) is just under 695,000 bytes [that is, excluding the covers].

In this case, a picture is worth much more than a thousand words.

⚡ Re: Cyber-terrorists blackmail banks and financial institutions

<[Identity withheld by request]>

Wed, 05 Jun 1996

>> Personally, I view this story with marked scepticism. I have no
>> doubt that it is true to a certain extent, but the idea of banks
>> forking out ten million pounds (circa \$14m [sic]) to a
>> blackmailer is one I find slightly unrealistic.

I have in the past done computer security work for several large banking institutions which everyone has heard of. In my opinion, with respect to the business case of choosing to pay blackmail or fix the problem, it is cheaper to make a few blackmail payments than to protect an entire multinational (or even single-nation) banking organization with strong information security (cryptography, of course). This is probably true even with five "cyber terrorist" organizations operating, but this obviously does not scale well.

This is, of course, disappointing (especially speaking as

someone who might attempt to make all that money legitimately designing security systems). However, I don't find it surprising at all. One blackmail payment of this level approximates the daily operating expenses of one of these organizations. Consider this loss alone, ignoring the lost profits and public relations nightmare, and you might pay the blackmail, too.

What these banks are surely not considering is that there are many other advantages to strong information security. Some banks are considering this, but not quickly enough, IMHO.

I've believed for a long time that the people who need security most won't do anything until they personally feel some intense pain. (This is analogous to the multitude of people who didn't believe in regular backups until one of their disks crashed.) If there was another Barings which folded due to inadequate security instead of financial mismanagement, maybe then the banking industry would do something real, and stop complaining at how painful security was. An ounce of prevention, and all that.

Marc

[I have some private reports suggesting that the story in [RISKS-18.17](#) is largely overhyped, but no complete denials at this time. I hope someone will eventually set the record straight. PGN]

🔥 Fourth ACM Conference on Computer and Communications

Security

"M.K. Reiter" <mkr23@newton.cam.ac.uk>

Wed, 5 Jun 1996 12:05:43 +0100

Call for Papers
Fourth ACM Conference on Computer and Communications Security
Zurich, Switzerland
April 2-4, 1997

Sponsored by ACM SIGSAC

Papers pertaining to all aspect of computer security are solicited for submission to the Fourth ACM Conference on Computer and Communications Security. Papers may present theory, technique, applications, and practical experience on a variety of topics including access control, accounting and audit, applied cryptography and cryptographic protocols, authentication and authorization, data/system integrity, electronic commerce, intrusion detection, key management, privacy, protection of software and intellectual property, run-time system security, secure networking, secure operating systems, security architectures and models, security management, security of distributed systems and databases, security protocols, and smart-cards and secure PDAs.

Instruction for authors: Papers should be of high quality, original, unpublished, and not submitted elsewhere. Submit six (6) copies of your paper (not exceeding 7500 words or 25 pages) to Clifford Neuman at the address below in a form suitable for anonymous review (no author names, affiliations, obvious references), with a cover letter

indicating that your paper is a submission for the ACM Conference on Computer and Communications Security, and listing the authors names, email and postal addresses, phone and fax numbers, and identifying the contact author. Electronic, faxed, or late submissions will be rejected without review. Send also via email bcn@isi.edu an online plain ASCII text version of your paper title, abstract, and authors and contact information. Where possible all further communications to authors will be via email.

Paper submission: September 2, 1996
Acceptance decision: October 21, 1996
Final papers due: December 9, 1996

Steering Committee Chair:
Ravi Sandhu, George Mason University, USA

General Chairs:
Richard Graveman, Bellcore, USA
Phil Janson, IBM Zurich Research Laboratory, Switzerland

Program chairs:

Clifford Neuman (4th ACM CCS)
University of Southern California
Information Sciences Institute
4676 Admiralty Way
Marina del Rey, California 90292-6695
U.S.A.
Tel: +1 (310) 822-1511
Fax: +1 (310) 823-6714
Email: bcn@isi.edu

Li Gong
SRI International
Computer Science Laboratory
333 Ravenswood Avenue
Menlo Park, California 94025, U.S.A.

Email: gong@csl.sri.com

Awards chair: Jacques Stern, ENS/DMI, France

Publication chair: Tsutomu Matsumoto, Yokohama National University, Japan

Publicity chair: Michael Reiter, AT&T Research, USA

Program committee members:

Martin Abadi, DEC Systems Research Center

Carlisle Adams, Bell Northern Research

Hugo Krawczyk, IBM T.J. Watson Research Center

Arjen Lenstra, Bellcore

Mark Lomas, University of Cambridge

Wenbo Mao, HP Labs, Bristol, U.K.

Tsutomu Matsumoto, Yokohama National University, Japan

Xiaolei Qian, SRI International

Michael Reiter, AT&T Research

Avi Rubin, Bellcore

Karen Sollins, MIT

Stuart Stubblebine, AT&T Research

Jacques Stern, ENS/DMI, France

Gene Tsudik, USC Information Sciences Institute

Vijay Varadharajan, University of Western Sydney

Michael Waidner, IBM Zurich Research Laboratory

Raphael Yahalom, Hebrew University, Israel

Moti Yung, IBM T.J. Watson Research Center

For more information, access <http://www.csl.sri.com/acm-ccs/ccs.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 18: Issue 19

Monday 10 June 1996

Contents

- [Janet Reno Wants Protection from Cybercrime](#)
[Edupage](#)
- [Martinair B767 Aircraft suffers EFIS failure](#)
[Peter Ladkin](#)
- [HTTP cookie privacy risk](#)
[Howard Goldstein](#)
- [Autodeletion](#)
[Bradley K. Sherman](#)
- [RISKs of dumb string searches](#)
[Gianfranco Boggio-Togna](#)
- [Matra made software for Ariane 5 AND Taipei subway system](#)
[Frank Rieger](#)
- [Re: The European Space Agency's little problem](#)
[James Brady](#)
[Marc Horowitz](#)
- [Re: L-Vis Lives](#)
[Matt Ackeret](#)
- [Virtual image tinkering, a positive side?](#)
[Mike Gardiner](#)
- [Digital unreality](#)

[Harold Asmis](#)

● [Re: College Paper Sued Over Quote](#)

[Nevin Liber](#)

● [Confusing cost with worth](#)

[Mike Albaugh](#)

● [1-week course on Internet Security, 29 Jul-2 Aug, at Stanford](#)

[Arthur Keller](#)

● [Formal Methods Europe Conference: Call for Papers](#)

[Cliff B Jones](#)

● [Info on RISKS \(comp.risks\)](#)

✂ Janet Reno Wants Protection from Cybercrime (Edupage, 6 June 1996)

Edupage Editors <educom@elanor.oit.unc.edu>

Thu, 6 Jun 1996 18:48:55 -0400 (EDT)

Attorney General Janet Reno has told the FBI, CIA, and Commerce, Defense,

Energy, Transportation and Treasury Departments that she wants to create a

federal computer security emergency response unit to counter physical or

network attacks against the federal computer infrastructure

(*Computer

Industry Daily*, 6 Jun 1996). And some U.S. senators want to allow the FBI

to combine forces with the CIA and other intelligence agencies to deal with

international criminal and terrorist activity conducted on the Net. Senator

Sam Nunn (D-Ga.) says that "if we're going to live in this kind of world,

we're going to have to link the intelligence world with law enforcement."

Vanderbilt business professor Donna L. Hoffman, whose work is focused on the

Internet, says: "There are not dead bodies in the street. It

just doesn't
make sense to rush into legislation.' ' (San Jose Mercury News*,
Center, 6
Jun 1996)

✈ Martinair B767 Aircraft suffers EFIS failure

Peter Ladkin <ladkin@TechFak.Uni-Bielefeld.DE>

Fri, 7 Jun 1996 21:25:13 +0200

Flight International (5-11 June 1996, p8) reports that the crew of a Martinair B767-300 registration PH-MCH `faced blank flight-instrument displays' near the US coastline on a flight from Amsterdam to Orlando, FL on 28 May 1996. Apparently it had suffered an EFIS failure (EFIS is the industry acronym for the system which displays the flight data on screens in front of the pilots -- a feature of most modern transport aircraft.

The EFIS failure itself was not such a big issue. The plane continued on the electro-mechanical standby instruments and diverted to Boston, where it landed safely -- but very fast, with no flaps, spoilers, autobrake or anti-skid. It burst 8 mainwheel tires and the brakes caught fire (neither event unusual in a fast landing and heavy stop) and the fire was quickly extinguished. Martinair said the crew employed `flaps one', which extends leading-edge spoilers only, and that they had no reverse thrust.

Martinair said the aircraft had a partial DC-power failure, but an unnamed 767 captain apparently said that such an event would not cause

an EFIS failure. Boeing said reports of a complete power failure are `not confirmed'.

Peter Ladkin

⚡ HTTP cookie privacy risk

Howard Goldstein <hgoldste@bbs.mpcs.com>

8 Jun 1996 01:38:13 GMT

I recently installed Netscape 3.0b4, a beta version, to try out the new (compared to 1.1N) features and see how well FreeBSD runs foreign binaries.

One of the new features, a security feature strangely categorized as a 'network' feature, queries the user before allowing "cookies" to be set.

Out of curiosity I set it so as to find out how often this feature was invoked. Cookies (discussed in earlier RISKS volumes, I seem to recall)

[YES: [RISKS-14.36](#), 17.89. PGN] are documented at http://www.netscape.com/newsref/std/cookie_spec.html .

I was surprised to find that every night for the last two weeks after enabling this I've been handed a "cookie" by a site I never knowingly visited, at <http://ad.doubleclick.net> .

Upon visiting this site I discovered they engage in attempts to collect various data about web users including their o/s. Why they feel it necessary to 'ping' me each night to set a cookie I do not know,

but it seems they are also collecting data about browser usage. Such a statistic regarding times online while in a browser would seem valuable from a marketing standpoint.

While cookies may be useful when voluntary and insofar as they may be helpful to the user (as I feel the cookie I'm handed that avoids an access validator for a particular newspaper's site). Cookies from marketing companies benefit me not.

Categorize this as a risk to users of older netscapes lacking the conditional-cookie setting? Or to advertisers who will find their targets are hidden behind "mini" HTTP firewalls that hide the users from cookies along with advertisement filter such as the one being tested by a North Carolina startup?

Howard Goldstein <hg@n2wx.ampr.org>

[And you'd probably be surprised to know how many people are affected.

But you *know* there has to be a gotcha with free web sites and free

browsers, and lots of folks are selling lists. Always look a gift

Trojan horse in the mouth (and everywhere else too). PGN

Autodeletion

Bradley K. Sherman <bks@netcom.com>

Mon, 10 Jun 1996 15:36:15 GMT

[found at <http://www.educom.edu/>]

The UNGAME

Irvine, California-based DVD Software has a new product that automatically deletes games from networked computers, freeing up limited computing resources for students and business folks. Oregon State University's business school manager says, "I had a problem with games," noting that some students spent hours playing games while others were waiting their turn at the keyboard to complete assignments. UnGame scans the hard drive for any of 4,600 games every time the computer is turned on or logged on to the network. The list of games is updated every month. More than 20 colleges and universities are using the software now. (*Chronicle of Higher Education*, 7 Jun 1996, A24)

--bks

[So, be careful how you name your programs.
Here are 4,600 UnNames not to use! PGN]

RISKs of dumb string searches

<G.Boggio@agora.stm.it>

Sun, 9 Jun 96 20:50:20 GMT

The RISKs of relying on dumb string searches are not confined to the mangling of respectable British town names ("AOL censors British town names!", [RISKS-18.07](#)). Today I accessed the FAQ archives at Imperial College, London (sunsite.doc.ic.ac.uk) to check the date of the alt.usage.english FAQ. Looking at the directory listing I was astonished to see that the 250K+ file had shrunk to 1K. I downloaded the alleged FAQ and found that it contained an article posted to alt.usage.english.

The author

suggested that, because of its size, the FAQ should no longer be posted to the newsgroup, since "it is available on the WEB, by e-mail, and by ftp".

The message subject line was, not surprisingly, "alt.usage.english FAQ":

apparently it was enough to fool the archiving program into assuming that the article **was** the FAQ.

This would seem to open up interesting possibilities for anyone objecting to the contents of a FAQ and wishing to have it removed from the archive.

Gianfranco Boggio-Togna Milano, Italy gbt@acm.org

[R](#) [18.17](#) Matra made software for Ariane5 AND Taipei subway system ([R](#) [18.17](#))

Frank Rieger <frank@artcom.de>

Fri, 7 Jun 1996 10:58:23 +0100

The German newspaper **Tageszeitung** reports in its issue from 6 June 1996 (6/6/6!) that the software for the engine-controlling in Ariane 5 was made by the French company Matra Corp. This is the same company that made the software for the Taipei subway system that crashed on 3 June 1996 ([RISKS-18.17](#)).

First statements from DASA, ESA and ArianeSpace say, that there were 37 seconds after the start an movement of all engines in one direction, causing the Ariane 5 into an extreme flight position. This disrupted the main

structure of the vehicle and triggered an automated destruction mechanism.

Some seconds later the manual destruction from ground control was triggered by the flight security officer for redundancy. According to German press agency Deutsche Presse Agentur, one manager of the French space agency CNES stated that the computer has tried to compensate a nonexistent problem in flight control by making this massive move.

So, for me there are two possible reasons for the crash:

- * there was an sensor failure, transmitting false data about the external conditions (wind, flight position) to the control system, or
- * there was an real Software "glitch" causing the critical failure.

On the base of the information available now, I ask myself, why was there no mechanism to avoid the control computers' attempt to go into this extreme flight position?

Frank Rieger

Added note, Date: Fri, 7 Jun 1996 17:39:19 +0100

As I have read now, the leading European TV-Satellite corporation ASTRA

has chosen Matra Corp. as hardware/software supplier for their next

generation of digital broadcast satellites... (Source: Deutsche Presse

Agentur). I think we will have a lot of fun watching TV in the next

years... Frank

[They seem to be developing a real Matra-archy!
Next they might do a Matra Metro. PGN]

✈ Re: The European Space Agency's little problem (Wood, [RISKS-18.18](#))

"James Brady" <jlbc@eci-esyst.com>

10 Jun 1996 11:17:05 -0400

David Wood suggested some form of parachute ejection and recovery system for payloads. The usual problems with this scheme are weight, cost, and complexity. Mercury and Apollo had launch escape systems to pull the capsule off the top of the launch vehicle either on the pad or during early flight. These systems were jettisoned on the way up to improve flight performance (get rid of the weight penalty.)

The Challenger disaster reminded us all of how useful such systems are for saving crew. Launch escape mechanisms to get the shuttle away from the external tanks and solid boosters on the pad and in flight were scrapped early due to the weight and complexity penalties, not to mention some valid safety concerns. (The Space Shuttle can actually abort during launch under specific conditions and return to the landing strip at Kennedy, or go on to a down-range site, or ditch in the ocean. Had sensors been available to tell the crew or ground controllers of the burn-through problem, one of these abort modes might have been employed with the chance of saving the crew if not the vehicle.)

To my knowledge, no launch vehicle intended to orbit an unmanned payload has

carried a launch-phase recovery system. Ariane 5 is a heavy lift vehicle, making a structure to hold the payload through a separation event, thrusting away from the vehicle, chute deployment, and splashdown in the Caribbean/Atlantic would be a marvel of a vehicle itself. I am not convinced parachutes could even be made to handle the weight of an Ariane 5 payload. And individual recovery systems for the "n" individual satellite payloads just multiplies the complexity by "n."

Adding launch-phase recovery systems to expendable launch vehicles would further increase launch costs not only for the mechanisms but for the down-range recovery personell and facilities that would be required for each flight, just in case. Launch costs are already so high as to stifle commercial development of space. Re-usable, robust launch vehicles like the DC-X, X-33, etc. promise to reduce launch costs and offer some advantages in these areas.... Witness the successful landing of the DC-X after an engine explosion (my memory fails me as to when in the flight test program this was).

Launch vehicle failures will occur, as do failures in any complex system. Until someone finds a way to get into space other than by riding atop a controlled explosion, there is only so much risk avoidance you can do. And from then on it's risk management. Taking a "free" ride on a new launch vehicle is a higher risk than buying a ride on a "proven" launch vehicle. But if you can't afford the ticket, you must decide if the risk of failure

is worth the scientific/commercial/political rewards of success.

On the other extreme, I remember NASA taking heat in the Apollo days for the fact that the first Saturn launch carried a few tons of sand into orbit rather than risk any useful payload on an unproven vehicle.

Jim Brady Raytheon E-Systems

✶ Re: The European Space Agency's little problem (Wood, [RISKS-18.18](#))

Marc Horowitz <marc@MIT.EDU>
Sat, 08 Jun 1996 21:31:59 EDT

I'm not sure if they had a parachute did or not, but there was planning and engineering work done to try to rescue the crew under certain failure modes, although this did not help the Apollo 1 astronauts.

Apollo carried more valuable cargo than any commercial rocket. Remember, it was the Apollo astronauts who forced NASA to design a window into the capsule, at a very high cost. The political and psychological costs of losing anyone, especially highly, expensively trained astronaut-heroes, are very high, and can therefore support safety features which would not make it into an unmanned craft.

>> What a risk - millions of (pounds, dollars, whatever - big in anyone's
>> currency) and all that work.

Designing a "separate and chute" mechanism into the Ariane 5

would be a neat engineering feat, but is it cost-effective? All rocket cargo is insured (and I'm sure the insurance is not cheap). If there was an advantage to this system, I expect either the insurance companies would fund it so they would have to pay off less often, or the aerospace companies would fund it to lower their premiums. It all comes down to economics in situations like this.

It is, as they say, only money, even if its quite a lot of it.

Marc

✈ Re: L-Vis Lives ([RISKS-18.18](#))

Matt Ackeret <mattack@eskimo.com>

Sat, 8 Jun 1996 01:23:39 GMT

I'm not saying that they won't be able to perfect the system, but at the moment, from the demo I saw on a news report about this system, it's really lame_. The idea is fairly impressive -- presumably they're doing 3D rotations and scaling of their advertizement in real time to then be shown on the ad area. The basic "how to get it on the screen" technology is simply regular old green screen chroma key that has been around for a long time. The impressive part is, repeating myself, making sure the ad "looks right" depending on the angle the camera is seeing it from.

Yet even with this, the ad placed in the green area was

jittering all over
the place. I was laughing at how cheezy it looked. It just
looked horribly
fake. Technically, it was actually that the ad _wasn't_
jittering exactly
with the camera, so for example the logo wouldn't be completely
centered (or
offset appropriately depending upon the angle) perfectly.
"Jittery" really
is the best word to describe it when you see the demo. I could
also see the
tell tale lines on the boundary showing it was chroma key. (They
also showed
the wall without the ad.. definitely regular old green screen
color.)

By the way, the idea that subliminal advertising actually works
is a
pernicious urban legend. Check out [http://www.urbanlegends.com/
products/](http://www.urbanlegends.com/products/)

[subliminal.advertising/subliminal_messages_sources.html](http://www.urbanlegends.com/products/subliminal.advertising/subliminal_messages_sources.html) for
several
references to books that fail to find any evidence that
subliminal
advertizing works. You may want to peruse [http://www.
urbanlegends.com](http://www.urbanlegends.com)
itself for info on lots of other things you probably believed to
be true but
aren't. (alt.folklore.urban's another good place.)

Virtual image tinkering, a positive side? (Re: L-Vis, [RISKS-18.18](#))

Mike Gardiner <mwg@conch.aa.msen.com>
Sun, 9 Jun 1996 20:13:42 -0400 (EDT)

With my mind always trying to find real uses for questionable
technology, I
find myself wondering if a home version of this technology could

be used in
reverse to delete those obnoxious logos that have done so much
to cut down
on how much TV I watch. Or better yet: Carl Sagan's AdNix chip
could
finally exist. Program it with every major corporate logo and
most ads
could be blacked. (Turnabout is fair play.) It would make a
mess of most
sporting events, though.

Mike Gardiner

✶ Digital unreality (was L-vis Lives in Virtual TV, [RISKS-18.18](#))

Harold Asmis <harold.w.asmis@hydro.on.ca>

Mon, 10 Jun 1996 10:17:08 -0400

This is merely an extension of a recent trend in digital
photography.
Articles in Scientific American, and others, have shown that
still pictures
can no longer be believed, since they are so easily altered.
Computer
technology now extends this to video (and live video, at that).

Now with digital camcorders, who will believe the next "Rodney
King" video
clip? Not enough cops? Add some more! It will probably boil
down to the
integrity of the picture-taker. We shall soon see all those
paragons of
virtue --tabloid TV&print, network television, etc-- swearing
that their
images have not been digitally altered in any way, except when
it brings in
more revenue. :-)

Harold W. Asmis harold.w.asmis@hydro.on.ca 416.592.7379 fax

416.592.5322

✦ **Re: College Paper Sued Over Quote (Wisneskey, [RISKS-18.18](#))**

Nevin ":-]" Liber <nevin@cs.arizona.edu>

Sat, 08 Jun 1996 07:27:40 -0700

> The risks? If you're going to have a generic template, make
> it generic.
> And if something bad happens once, it's going to happen again
> so fix it
> after the first occurrence.

I see the RISKS as more social than technical. Will this kind
of thing
happen in the future? Of course. Was it appropriate? No. Was
the
response of an \$850K lawsuit appropriate? Absolutely not. It
reminds me a
lot of the Carl Sagan vs. Apple Computer lawsuit, and we all
know how that
turned out (or, if you don't, check out
<[http://www.info.apple.com/pr/press.releases/1996/q1/951115.pr.
rel.sagan.html](http://www.info.apple.com/pr/press.releases/1996/q1/951115.pr.rel.sagan.html)>
).

Nevin ":-)" Liber

nevin@CS.Arizona.EDU

(520) 293-2799

✦ **Confusing cost with worth (Re: Koenig, [RISKS-18.18](#))**

Mike Albaugh <albaugh@agames.com>

Mon, 10 Jun 1996 10:01:00 -0700 (PDT)

In [RISKS-18.18](#), Andrew Koenig <ark@research.att.com> writes:

> Occam's Razor suggests a more general explanation: Images contain much more
> information than text, regardless of content.

I wouldn't quibble with his point that images contain more data. I do have a problem with the proliferation of a popular confusion that I am surprised to find coming from ATT. Claude Shannon long ago gave an excellent definition for "information" that relates it to "surprise" or perhaps "useful news". I submit that the average picture, especially on the Web, has a great deal less information than the accompanying text, in the sense that the picture rarely contains anything a) worth much to the viewer or b) not deducible from the text. In the case mentioned, with 695K (400 pages?) of "text" versus 306K of image data, I find it truly astonishing that the author would state:

> In this case, a picture is worth much more than a thousand words.

Does anybody really believe that someone would shell out the price of a very nice dinner (assuming without real basis that this is a technical book, and thus priced in the neighborhood of 50 USD :-)) for these two pictures? "Worth" must be used in some sense with which I am unfamiliar. Although the two pictures cost as much about 51000 words, or about 25K words apiece, they aren't worth as much.

As for RISKS, when the technical community buys into popular misconceptions, such as "data == information" or "No more could be done about the abysmal

reliability of commodity software", we are helping bring about the disasters we read about. An informed populace will be vital in the shaping of government response to the changes brought by computing. Repeating the mistakes of the un-informed will not bring this about.

Mike Albaugh (albaugh@agames.com) Atari Games (now owned by Williams)
675 Sycamore Dr. Milpitas, CA 95035 voice: (408)434-1709

✦ 1-week course on Internet Security, 29 Jul-2 Aug, at Stanford

Arthur Keller <ark@DB.Stanford.EDU>
10 Jun 1996 09:00:57 GMT

The Western Institute of Computer Science announces a week-long course on INTERNET SECURITY to be taught at Stanford University 29 Jul to 2 Aug 1996, headed by Arthur M. Keller (Stanford University), with 9 well-known folks. Try URL <http://www-wics.stanford.edu/WICS.html> or contact ark@DB.Stanford.EDU (Arthur Keller) for details.

✦ Formal Methods Europe Conference: Call for Papers

Cliff B Jones <cliff@cs.man.ac.uk>
Fri, 7 Jun 96 07:48:06 BST

FORMAL METHODS EUROPE
FME '97
International Symposium and Tutorials

15--19 September 1997

The Technical University of Graz, Austria
Sponsored by the Commission of the European Communities

Call for Submissions

The Technical University of Graz will host the fourth FME Symposium from 15 to 19 September 1997. It is being organised by Formal Methods Europe which is the advisory panel of the Commission of the European Communities. This will be the successor of six previous VDM and FME symposia which have been notably successful in bringing together users, researchers and developers of precise mathematical methods for software development.

The theme of FME'97 is Formal Methods: Their Industrial Application and Strengthened Foundations.

Symposium contributions will report advances in the field from developments in applicable theory to experiences in commercial application. The conference will also follow the previous successful pattern of offering tutorials, tools demonstrations, reports of industry usage and research papers.

Categories of Papers: three kinds of full-length paper are solicited:

1. reports on industrial usage;
2. research papers on existing methods (for instance: extensions, innovative case studies);
3. articles on stimulating theoretical research with clear potential applicability.

Authors are requested to mention the category (1, 2, or 3) of their papers

when they submit.

TOPICS

The scope of the symposium includes, but is not limited to, the following topics:

- * Practical use, case studies
- * Comparisons of existing formal methods, extensions, improvement
- * Theoretical foundations
- * Tool support
- * Specification and refinement techniques
- * Verification against specifications
- * Development process
- * Linking formal and informal methods
- * Concurrency, real-time and reactive systems
- * Secure or/and safety-critical systems
- * Object orientation
- * Education and technology transfer

Submissions are encouraged from the full range of application areas including medical systems, aerospace and avionics, telecommunication, traffic modelling and transportation systems, nuclear safety, process and off-shore industries.

TUTORIALS

There will be eight Tutorials, each lasting a half-day. They will be organised in two parallel tracks during 15 and 16 September. Proposals for tutorials are welcome.

TOOL DEMONSTRATIONS

Tool demonstrations will take place during the Symposium, with the opportunity for presentations to be made about each tool (video

projectors will be available). Proposals for tool demonstrations are welcome and should be made to the Organising Chair, with whom provision of necessary computing facilities should be discussed.

CHAIRS

Organising Chair: Peter Lucas, IST, Technical University of Graz, A-8010
Graz, Muenzgrabenstrasse 11/II, Fax: +43 316 841 7566, Tel: +43 316 873
5712, Email: lucas@ist.tu-graz.ac.at

Programme Co-Chairs:

* Cliff Jones, Dept. of Computer Science, The University of Manchester, UK,
Email: cbj@cs.man.ac.uk
* John Fitzgerald, Centre for Software Reliability, The University of Newcastle, Newcastle upon Tyne NE1 7RU, UK, Fax: +44 191 222 8788,
Tel: +44 191 222 7999, Email: John.Fitzgerald@ncl.ac.uk

Programme Committee:

Manfred Broy	Technical University, Munich
George Cleland	Harlequin
John Fitzgerald (co-Chair)	CSR, Newcastle University
Peter Froome	Adelard
Chris George	United Nations University IIST
Shinichi Honiden	Toshiba
Daniel Jackson	Carnegie-Mellon University
Cliff Jones (co-Chair)	Manchester University
Carlos Jose Pereira de Lucena	Computer Science Department PUC Rio de Janeiro
Doug McIlroy	Bell Laboratories
Brendan Mahony Organisation	Defence Science and Technology Australia
Lynn Marshall	Northern Telecom (Nortel)
Dominique Mery	University Henri Poincare & IUF
Peter D. Mosses	BRICS, University of Aarhus
Jose Oliveira	University of Minho

Nico Plat	Cap Volmac
Andrzej Tarlecki	Warsaw University
Martyn Thomas	Praxis, Deloitte & Touche Consulting Group
Rob Witty	GEC
Joakim von Wright	Abo Akademi University

Organising Committee:

Andreas Bollin (Tools Exhibition), Brigitte Froelich, Gabriele Leitner,
Richard Messnarz, Gerhard Pail (Accounting), Petra Pichler

Local Organization: Graz Tourismus Ges.m.b.H

SUBMISSIONS

All papers and proposals for tutorials should be sent the Programme
Co-chair, John Fitzgerald, at the address given above.

Proposals for tool demonstrations should be sent to the organising chair.

Submissions by electronic mail are not accepted.

Format of submissions:

* Full, original papers mentioning one of the three above categories

(5 copies, 20 pages max; following the LNCS format is mandatory; a

description of the format and Latex style files are available by anonymous ftp at [ftp.springer.de](ftp://ftp.springer.de) in directory /pub/tex/latex/llnsc or via the world-wide web in <http://www.springer.de>)

* Proposals for tutorials (1/2 day, maximum 50 pp of notes)

* Proposals for tool demonstrations (2 pages of presentation plus hardware and software requirements)

Important dates:

- * Deadline for submission: 17 January, 1997
- * Notification of acceptance sent to authors: 25 April, 1997
- * Camera-ready copy due to publisher: 20 June, 1997 (latest date of arrival in Newcastle)



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 18: Issue 20

Weds 12 June 1996

Contents

- [Federal Court KOs CDA](#)
[Marc Rotenberg](#)
- [The computer is always right - again](#)
[Richard S. MacDonald](#)
- [The Risks of *Zero Hour* by Joe Finder](#)
[Peter Wayner](#)
- [Re: L-vis Lives in Virtual TV](#)
[Barry L Gingrich](#)
[Eamonn McManus](#)
- [Digital photographic forgeries: nothing's ever new!](#)
[Scott Alastair](#)
- [Re: Digital unreality](#)
[Jason Eisner](#)
[Lauren Weinstein](#)
- [F-15 revisited again](#)
[David Damerell](#)
- [Ariane-5 failures](#)
[Bertrand Meyer](#)
[David Wadsworth](#)
- [RISKs of bogus FAQs](#)
[Tom Lane](#)

- [CFP: 1997 Symposium on Network and Distributed System Security](#)
[Matt Bishop](#)
 - [Re: HTTP cookie privacy risk](#)
[Kenneth Albanowski](#)
[Rob Streno](#)
[Scott Hazen Mueller](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ Federal Court KOs CDA

"Marc Rotenberg" <rotenberg@epic.org>
12 Jun 1996 18:15:34 -0500

In a ruling likely to have a significant impact on the future of the Internet, a special three-judge federal court today declared the Communications Decency Act unconstitutional on its face. The landmark decision came in a legal challenge initiated by the ACLU, EPIC and 18 other plaintiffs. EPIC is both a plaintiff and co-counsel in the litigation. The ACLU/EPIC case was consolidated with a subsequent action filed by the American Library Association and a broad coalition of co-plaintiffs.

Today's lengthy ruling consists of separate opinions authored by the three members of the federal court panel. While the three judges differed in their approaches to the legal issues raised in the case, they were unanimous in their strong conclusions that the CDA constitutes a clear violation of the First Amendment.

A complete copy of the opinion, as well as selected excerpts and related

news items, can be found at <http://www.epic.org/> .

Marc Rotenberg, EPIC

✶ The computer is always right - again

"Richard S. MacDonald" <dickmac@ix.netcom.com>

Wed, 12 Jun 1996 12:03:51 -0600

A major computer chain recently tried to charge me an exorbitant price for ZIP disks. The price was about 1.5 times what other stores are selling them for and about the same amount higher than the price listed on the tag on the shelf.

The manager was willing to sell me the disks at the shelf price but noted that they would have to change that since the computer said it was higher. I told her that their price tag was most likely to be right because of the comparison to other chains but she insisted that the tag must be wrong rather than the computer.

I wonder how many people paid \$62.96 for the package instead of \$45.96 or if they simply don't sell as many as their competition. I also wonder if computer stores are more or less likely than other stores to believe that the computer is in error.

Fortunately in this case there is another chain right across the street...

Richard S. (Dick) MacDonald

⚡ The Risks of *Zero Hour* by Joe Finder

Peter Wayner <pcw@access.digex.net>

Mon, 10 Jun 1996 23:30:13 -0400

The dust jacket copy for `_Primary Colors_` promises that the book will tell the truth in a way that only fiction can do. RISKS readers might enjoy a friend Joe Finder's novel `_Zero Hour_` for the same reason. The book is a crisp thriller that revolves around a high-tech hold up. Many of the plot twists are modern day extensions of *deus ex machina*. The characters assume that technology will do the right thing only to discover that they missed one fatal detail. Time and time again the plot zigs because of a topic that would be ripe for `comp.risks` if the book was only factual. Given that many fiction writers are often just rogues who wanted a presentable day job, we might be better off learning these lessons before the less law-abiding discover them and the twists become fact.

⚡ Re: L-vis Lives in Virtual TV ([RISKS-18.18](#))

Barry L Gingrich <gingrich@indra.com>

Mon, 10 Jun 1996 21:39:57 -0600 (MDT)

Think about the logical next step of combining L-Vis, Digital Cable, and Direct Marketing. (It's the sort of thing you almost don't want

to mention
because it just might come to pass... :-) In such a digital
world,
micro-marketing is possible. For example, consider a can of soda
in an
episode of the X-Files. Scully's soda appears to be a can of
SpiffyFizz
(tm) on my set ("Hey! My favorite!"), while my neighbor sees
Diet Kumquat
Royale, and someone across town sees her drinking a can of
Nietzsche Lite
Beer.

The possibilities are endless, of course. One effect could be
the denial of
the (doctored?) video image as evidence in court, something
that's been
predicted for quite some time now. Another could be the
crumbling of the
public's faith in the media, something that's also been
predicted for Quite
Some Time now.

As T Bone Burnett said, "I have a feeling that once something
appears in the
paper, it ceases to be true."

These are societal risks, not technical ones. They certainly are
gloomy
predictions, but this technology could provide some benefits as
well. For
example, a filmmaker could correct problems with a particular
scene (a la
what was done for a scene with Brandon Lee in "The Crow"),
obviating the
need for a reshoot. The technology has great potential for
abuse, but the
people who would abuse it are *people*, and the risk lies with
them. It's
much like the arguments over the 'net: Is it a pit of doom, a
pillar of
hope, or a useful tool?

There are many things that could go wrong, of course, and I'm sure the denizens of RISKS will collect ample examples of L-VIS wipeouts, screw-ups, and wacky unexpected behaviors.

Barry L. Gingrich gingrich@indra.com

✉ Re: L-Vis Lives in Virtual TV (Ackeret, [RISKS-18.19](#))

Eamonn McManus <emcmanus@gr.osf.org>

Tue, 11 Jun 96 11:00:23 -0400

In [RISKS-18.19](#), Matt Ackeret says, of the electronic insertion of advertisements into live video, that the system is "really lame" and "jitters all over the place", and that it uses "regular old green screen chroma key". This is plainly not the same system that I saw a report on in February on French TV. In that report, they showed images from the Open Gaz de France as broadcast in France and in Germany. The French images were untouched but in the German ones a French ad behind one of the players was replaced by an equivalent German one. The substitution was *absolutely imperceptible*, and this even though the field being replaced was not a simple green rectangle but an ad in black on white.

The report mentioned that the system had been developed by a French company, so it is presumably not the same as the Princeton Video Image system mentioned by PGN. The image processing is done by a bank of equipment in a small truck on site. It may be that the TV standards (PAL and

SECAM) used
in Europe lend themselves more easily to this kind of treatment
than the US
standard.

Eamonn McManus Grenoble, France <emcmanus@gr.osf.org>

✶ Digital photographic forgeries: nothing's ever new!

"Scott Alastair (Exchange)" <ScottA@logica.com>

Tue, 11 Jun 1996 09:27:58 +0100

Tampering with images has been done, I would suspect, ever since
the
birth of photography: I can think, off the top of my head, of a
number
of cases from well before the age of computer imaging:

(i) Retouching of facial features to make family members appear
villainous (1911);

(ii) Removal of Trotsky from a picture, plus many other similar
forgeries (1928);

(iii) Removal of Soviet astronauts from group photographs when
they
fell out of favour (1950s and 1960s).

The first was part of a study by Goddard on the heredity of IQ
and has
been exposed in Stephen Jay Gould's essays; the second is well-
known (a
photo of Lenin haranguing a crowd from a lectern with Trotsky
[not]
standing at the bottom of it); I wish I could get hold of the
book
again in which I saw the third, where astronauts were replaced by
strategically-placed rose bushes, doors etc. etc.

This whole thread illustrates a common misattribution: evils

attributed to
the baleful influence of computers were actually practiced well
before
computers could help perpetuate them!

Come to think of it, the whole area of digital and "analogue"
photographic
forgery is so interesting it almost demands to have a book
written about it.

✶ Re: Digital unreality (Asmis, [RISKS-18.19](#))

Jason Eisner <jeisner@unagi.cis.upenn.edu>

Tue, 11 Jun 1996 12:51:02 -0400

> Now with digital camcorders, who will believe the next "Rodney
King" video
> clip? Not enough cops? Add some more! It will probably boil
down to the
> integrity of the picture-taker.

Or the integrity of the camcorder. Any digital camera --
certainly any
camera used for police work or journalism -- ought to sign its
output with a
factory-installed private key.

(If the camera is not robustly tamper-proof, someone might
extract the
private key by reverse engineering, or diddle the innards of the
camera so
that the image is optically or digitally altered before being
signed.
However, if each camera has a different private key, a court can
check for
an unbroken seal on the one that purportedly shot and signed the
picture.)

Jason Eisner University of Pennsylvania

⚡ Re: Digital Unreality

Lauren Weinstein <lauren@vortex.com>

Tue, 11 Jun 96 10:54 PDT

It appears that image tinkering to create lies is now considered to be a mass-market product selling point. In a national television commercial from a *major* PC manufacturer that seems to have just started airing, a "nerd" who finishes a marathon long after everyone else (in over 9 hours), upon learning that someone is coming over to visit, immediately scans the photo of himself and the marathon clock, changes the leading "9" to a "2", and prints it out. He then proceeds to burn his mouth on a piece of pizza.

--Lauren--

P.S. The pizza lends an air of authenticity, but would the nerd have even run the marathon in the first place?

⚡ F-15 revisited again

David Damerell <djsd100@thor.cam.ac.uk>

Tue, 11 Jun 1996 10:53:15 +0100

> - (To my disbelief) It was suggested some type of plastic cap
> be placed on the main trigger during future training missions
> to

> prevent pilots from triggering(!?).
>The last low-tech solution to the prevention of triggering the
missile
>was almost comical.

Comical and low-tech, perhaps, but it would work. Sometimes a
visible
physical barrier is superior to any number of invisible things
which
should have been done right...

✈ Ariane-5 failures

Bertrand Meyer <bertrand@vienna.eiffel.com>

Fri, 7 Jun 96 10:07:42 PDT

[>From Le Monde, dated 8 June 1996, i.e. published on the 7th;
on-line
edition at <http://www.lemonde.fr>. Extracted and translated by
BM.

(Although ellipses are not marked, I have considerably
abbreviated the
text and removed some of the anthropomorphic comments, e.g.
"the machine's
brain" and the like. Comments in square brackets [] by BM.))

THE MYSTERIES OF ARIANE'S CHAMBER, by Jean-Francois Augereau

Who [sic] caused the in-flight explosion of Ariane-5 on Tuesday,
June 4?
After more than forty-eight hours of preliminary investigations,
"witnesses"
are starting to talk. The propulsion system, which could have
been
suspicious because of its novelty, has been cleared. The likely
culprits are
elsewhere, "in the software or the hardware", that is to say the
computer-related parts. Only five of them are left, gathered in
one "closed

room". [???

According to Daniel Mugnier, head of the Launchers ("lanceurs") division at the CNES (National Center for Aerospace Studies), the inquiry is focusing on the "electrical and software system" which allows the various elements of Ariane-5 to talk to each other. The launcher is loaded with sensors which constantly monitor its moves and accelerations.

Our first suspect is an Inertial Reference System (IRS)*, the balancing center of the launcher. The IRS, or its mate, is in charge of using these data to compute the launcher's exact position, speed and acceleration. But at this stage of the inquiry it seems that the sensors themselves have been exonerated.

There is no alibi, however, for the IRS. Doubts remain, even though the on-board computer and the backup unit show a record of having received [litt. "claim to have received"] the same information. How could they have failed at the same time and in the same way?

Hence the questions about the behavior of on-board computers. According to Daniel Mugnier, "they ``claim'' to have received abnormal information from the IRS. Whom [sic] should we believe? Daniel Mugnier is reluctant to incriminate that component [i.e. the computers?]. Same thing with another component, the "1553 bus". It is a kind of information highway [??!!]; all navigation commands go through it. According to one of the investigators, "it is a proven system, which has been used for a long time on

all NATO
fighter planes".

This leaves two other suspects: the in-flight software program and the coder. Does the program, made of long lines [???] of computer writing, include a "bug" or a fault? Did the converter**, which translates the sensors' analog language into the computers' digital language, stutter? One cannot exclude the possibility that the computer is denouncing errors that it itself created.

The investigation continues. The report should be turned in by July 15.

[Notes:

* I have translated "Centrale Inertielle (SRI)" by "Inertial Reference System (IRS)". I found the acronym in Jane's Defence Glossary at <http://www.thomson.com/hanes/janesgloss>. I don't believe it's directly connected to the Internal Revenue System.

** I used "converter" for the analog-to-digital "codeur".]

Bertrand Meyer
ISE Inc., Santa Barbara, <bertrand@eiffel.com>, <http://www.eiffel.com>

Ariane-5 failures

David Wadsworth <dwadsw@etna.demon.co.uk>
Fri, 07 Jun 96 17:40:28 GMT

An interesting feature of the Ariane 5 explosion, as seen on television, was

the commentary in French in the background. As the fragments of the destroyed rocket were coming down, the French voice was still saying the equivalent of "All systems go", "All parameters normal" "course correct" etc. I suppose the risk of a commentator reading from a script describing what *should* be happening is obvious. At least they could have given him a window or a monitor to check that it loosely coincided with reality!

David Wadsworth dwadsw@etna.demon.co.uk

⚡ RISKs of bogus FAQs (Boggio-Togna, [RISKS-18.19](#))

Tom Lane <tgl@netcom.com>
Mon, 10 Jun 96 23:10:23 -0700

> This would seem to open up interesting possibilities for anyone objecting
> to the contents of a FAQ and wishing to have it removed from the archive.

I maintain another such FAQ article. Most of the FAQ archive sites that I know about will archive any article that comes by, if it (a) is crossposted to news.answers and (b) contains the appropriate headers, such as the proper Approved: line and Archive-Name: line. Of course, these conditions are trivially easy to forge for anyone familiar with the workings of netnews transport software. (In fact, the standard posting software most FAQ authors use requires no special system privileges; you could say that we

all forge these headers.) So far, there hasn't been any concerted attack on FAQ archives, but I'm sure there will be one someday ... and that nothing will be done to plug the security holes until an incident occurs :-(. The archive site Gianfranco describes seems to have laxer security than average, but there isn't any trustworthy system in place.

My own FAQ is several posting cycles out of date in most of the FAQ archive sites, and I think that Risks readers might be interested in the reasons why. I normally post my FAQ every other weekend. Four weeks ago, the posting got lost due to failure of the local netnews system at netcom.com. Two weeks ago, it went out OK, but that weekend some self-appointed vigilante decided to shut down the alt.binaries.* newsgroups by issuing forged cancels for every article posted or crossposted to any alt.binaries.* group. My FAQ is crossposted to several .d (discussion) groups under alt.binaries.*, and it got canceled before being archived at most sites. The vigilante was toast a couple days later, of course, but the damage was done. The most recent posting is hung up in our outgoing news queue due to another local news system failure. Perhaps it will eventually get out, or perhaps not.

Meanwhile, the single most popular FAQ archive site (ohio-state.edu's WWW-accessible archive) has had ongoing reliability problems because its volunteer founder and administrator left Ohio State over a year ago, and everything is running on autopilot. There are other

regularly
posted FAQs that are more out of date in ohio-state's archive
than mine.

The RISK: things you would think are bedrock Internet services
may
actually be unfunded volunteer projects full of security holes.

Another example I've recently been reading about is that a
couple of the
root DNS nameservers have been down for several days. If they
all go down,
the Internet as we know it comes to a stop. Yet the
administration of these
critical services is run on an ad-hoc, volunteer basis. Sooner
or later,
the net will have to grow up and take itself seriously.

Tom Lane

✶ CFP: 1997 Symposium on Network and Distributed System Security

Matt Bishop <bishop@cs.ucdavis.edu>

Fri, 07 Jun 1996 13:13:36 -0700

CALL FOR PAPERS [abridged for RISKS]
The Internet Society Symposium on
Network and Distributed System Security

February 10-11, 1997, San Diego Princess Resort, San Diego,
California

Submissions due: August 1, 1996

GOAL: The symposium will bring together people who are building
hardware
and software to provide network and distributed system security
services.

The symposium is intended for those interested in the practical

aspects of network and distributed system security, focusing on actual system design and implementation, rather than theory. We hope to foster the exchange of technical information that will encourage and enable the Internet community to apply, deploy, and advance the state of available security technology.

Symposium proceedings will be published by the IEEE Computer Society Press.

Topics for the symposium include, but are not limited to, the following:

- * Design and implementation of communication security services: authentication, integrity, confidentiality, authorization, non-repudiation, and availability.
- * Design and implementation of security mechanisms, services, and APIs to support communication security services, key management and certification infrastructures, audit, and intrusion detection.
- * Requirements and designs for securing network information resources and tools -- WorldWide Web (WWW), Gopher, archie, and WAIS.
- * Requirements and designs for systems supporting electronic commerce -- payment services, fee-for-access, EDI, notary -- endorsement, licensing, bonding, and other forms of assurance.
- * Design and implementation of measures for controlling network communication -- firewalls, packet filters, application gateways, and user/host authentication schemes.
- * Requirements and designs for telecommunications security especially for emerging technologies -- very large systems like the Internet, high-speed systems like the gigabit testbeds, wireless systems, and personal communication systems.

- * Special issues and problems in security architecture, such as interplay between security goals and other goals -- efficiency, reliability, interoperability, resource sharing, and cost.
- * Integration of security services with system and application security facilities, and application protocols -- including but not limited to message handling, file transport, remote file access, directories, time synchronization, data base management, routing, voice and video multicast, network management, boot services, and mobile computing.

GENERAL CHAIR:

David Balenson, Trusted Information Systems

PROGRAM CHAIRS:

Clifford Neuman, University of Southern California

Matt Bishop, University of California at Davis

All submissions and program related correspondence (only) should be directed to the program chair: Clifford Neuman, University of Southern California, Information Sciences Institute, 4676 Admiralty Way, Marina del Rey, California 90292-6695, Phone: +1 (310) 822-1511, FAX: +1 (310) 823-6714, e-mail: sndss97-submissions@isi.edu. Dates, final call for papers, advance program, and registration information will be available at the URL: <http://www.isoc.org/conferences/ndss97>.

✶ Re: HTTP cookie privacy risk (Goldstein, [RISKS-18.19](#))

Kenneth Albanowski <kjahds@kjahds.com>

Tue, 11 Jun 1996 16:18:20 -0400 (EDT)

This site makes very interesting reading, as does an AltaVista search for "ad.doubleclick.net", as does my ~/.netscape/cookies file, which contains a reference to ad.doubleclick.net.

It appears that anyone can set up with "DoubleClick.net" (for a fee) so that access to their own web pages goes through DC.net. DC.net then returns the original web page, with targeted advertising added, based on the information that some web browsers hand out on every fetch operation.

It's unclear exactly how the cookies come into this, but they undoubtedly let DC.net try and target individual preferences, probably based on what pages they read that go through DC.net.

The interesting thing is that this is all completely invisible, unless you happen to notice having a cookie for ad.DC.net, or have a habit of reading through HTML code and see an odd URL that points to ad.DC.net. Most people would never see these.

Thus does modern marketing come to the WWW. The risks here are enormous. The solutions, to some extent, are simple -- no hidden cookies, and no personal information getting sent out without approval. You can't very well hide your domain, however, and that lets people guess all sorts of fun things. The solution to that is not so simple.

Kenneth Albanowski (kjahds@kjahds.com, CIS: 70705,126)

✂ Re: HTTP cookie privacy risk (Goldstein, [RISKS-18.19](#))

Rob Streno <rstreno@dayton.csc.com>

Tue, 11 Jun 1996 16:18:28 -0400

You've been visiting commercially sponsored sites, haven't you. Doubleclick is responsible for the ads that you see on pages such as the DejaNews search engine (<http://www.dejanews.com>) are linked via DoubleClick to the destination site.

As far as privacy risks go, if I remember, the Netscape documentation about the cookie file indicates that it is a file to be used to hold information from one page to the next. . . i.e., one page writes the cookie, and another page reads it. This keeps from having long, convoluted URL lines which contain all of the information you need to pass from page to page.

As far as gathering marketing information, I can't fault DejaNews, Doubleclick, or any other company for gathering marketing information. My guess is that they'll use that information to tailor which ads are most effective to display on a page like DejaNews. I doubt that they'll use that information to direct market you via e-mail.

Robert M. Streno rstreno@dayton.csc.com (513) 890-7700 x2455
rstreno@csc.com xinc@ix.netcom.com xinc@delphi.com

✂ Re: HTTP cookie privacy risk

Scott Hazen Mueller <scott@zorch.sf-bay.org>

Tue, 11 Jun 1996 22:18:17 GMT

DoubleClick is a Web advertising agency. They buy space on Web sites (Yahoo, Netscape, Travelocity, etc.) and sell impressions ("eyeballs") to advertisers.

While they may or may not actually care about your particulars (and your browser/OS information is available to any Web site that cares to gather it, regardless of cookies), it's much more likely they're just tagging you, like a biologist tags wild birds.

Ideally, it's a trade-off, you see. In exchange for free information (quid), you give a little information on your Web usage (pro quo). In a RISKy world, the concern is that you give up too much for too little. As a person who cares about privacy, I have to applaud Netscape for putting a little alert about cookies on the users screen. As a Web site maintainer, I have to wonder if this is going to affect my ability to deliver advanced forms of content.

Scott Hazen Mueller | scott@zorch.SF-Bay.ORG or tandem!zorch!
scott



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 18: Issue 21

Monday 17 June 1996

Contents

- [Whitehouse Namechecks Glitch](#)
[David Kennedy](#)
- [UK government announces proposals for encryption on networks](#)
[Steve Kilbane](#)
- [Korea's Internet War](#)
[David Kennedy](#)
- [Health Risk from Dusty Computer Displays](#)
[Martin Minow](#)
- [Botched trademark search](#)
[George C. Kaplan](#)
- ["Child Molester Database" on the Web](#)
[Dave Brown](#)
- [Magellan 3000 GPS is `waterproof`?](#)
[Boyd Roberts](#)
- [Rounding errors and grammar checkers](#)
[Gabor Megyesi](#)
- [Re: Digital unreality](#)
[Lauren Weinstein](#)
[Luis Fernandes](#)
- [Re: Ariane-5 failures](#)

[Lauren Weinstein](#)

● [Physical barriers in the cockpit](#)

[Karl W. Reinsch](#)

● [French police raid leading ISPs](#)

[Jean-Bernard Condat](#)

● [Info on RISKS \(comp.risks\)](#)

⚡ Whitehouse Namechecks Glitch

David Kennedy <76702.3557@CompuServe.COM>

13 Jun 96 14:02:48 EDT

Courtesy of Associated Press via CompuServe's Executive News Service:

AP US & World 12 Jun 1996

FBI Files

By PETE YOST

Associated Press Writer

>> WASHINGTON (AP) -- Whitewater prosecutors have questioned
>>before a grand jury the Army employee who led the White House
>>collection of FBI background files on a number of prominent
>>Republicans. [...]

>> FBI officials investigating how the White House obtained the
>>files have tentatively concluded that FBI procedures were not
>>adequate to prevent the improper disclosure of personnel
>>reports, The New York Times reported in today's editions,
>>quoting unnamed government officials. [...]

>> In addition, the newspaper quoted a senior career government
>>employee as saying the computer program the Secret Service used
>>in 1993 to track access to the White House was flawed,
>>producing an outdated list. [...]

>> "What is remarkable is that in this case an outdated list
>>was being used so unnecessary files were retrieved," said White
>>House spokesman Mark Fabiani.

[DMK: The computer did it! It's not my fault! (sigh)]

Dave Kennedy [CISSP] Information Security Analyst, National Computer Security Assoc.

[Lengthy articles in the *NY Times* and the *Washington Post* over the weekend noted the distinction between the "A" and "I" tags for active and inactive names on the list. A Secret Service spokesman was quoted as saying that it was impossible for the I list to appear without the tags, although a query that did not request that field would omit them because it was indicated that both lists were in the same (relational?) database. As usual in such cases, the "blame" may be distributed much more widely than folks like to admit, or alternatively may be attributed to a lack of understanding of the technology. Stay tuned. PGN]

🚀 UK government announces proposals for encryption on networks

<Steve_Kilbane@cegelecproj.co.uk>

Thu, 13 Jun 1996 09:54:39 +0100

On 10th June, the UK government announced a document which describes a key-escrow system. The document is available at:

<http://www.coi.gov.uk/coi/depts/GTI/coi9303b.ok>

I'm not going to get into the usual arguments. I will quote the

following,
however:

"2. The policy, which has been decided upon after detailed discussion between Government Departments, involves the licensing and regulation of Trusted Third Parties (hereafter called TTPs) which will provide a range of information security services to their clients, whether they are corporate users or individual citizens. The provision of such information security services will be welcomed by IT users"

Not by this one, they won't.

🔥 Korea's Internet War

David Kennedy <76702.3557@CompuServe.COM>
14 Jun 96 21:09:44 EDT

Courtesy of Associated Press via CompuServe's Executive News Service:
AP US & World 14 Jun 1996

Korea's Internet War
By SANG-HUN CHOE, Associated Press Writer

>> SEOUL, South Korea (AP) -- For a Canadian university student,
>>creating an Internet site on North Korea was simply opening a
>>small library on the reclusive nation. For South Korean
>>authorities, it was threat to national security.
>> Last week, South Korea declared David Burgess' World Wide Web
>>site subversive and ordered 14 local computer networks with
>>Internet links to block public access to it.

- o Government plans to punish those accessing PRNK web sites.
- o About 0.5M South Koreans are plugged in.

>> "South Korea has hypocritically committed the same actions
>>it criticizes North Korea for -- non-promotion of democratic
>>values and open choices," Burgess said in an electronic mail
>>message to The Associated Press.

o Burgess visited PRNK and picked up some pamphlets, which
he's now
 posted to his web server.

>> North Korean pamphlets found on Burgess's home page are
>>sprinkled with references to the "Greatest Genius Mankind Has
>>Ever Known, Comrade Kim Jong Il," "U.S. imperialist warmaniacs"
>>and "South Korean puppet reactionaries."

>> They might be laughed off as Cold War classics, but under
>>South Korea's strict national security law, it is a serious
>>crime to "manufacture, import, copy, possess or distribute data
>>that can benefit, eulogize or encourage the enemy."

o ROK jams the PRNK's HF radio stations.

o A ROK official admitted their regulations are not very
effective and
 that, "(w)e need a new approach."

>> The government has its own web sites promoting its policies
>>and chronicling the doings of President Kim Young-sam. But it
>>maintains a sweeping ban on communist propaganda.

>> About 340 people are in prison for breaking the law,
>>according to human rights groups. None were arrested in
>>connection with Burgess's home page.

>> EDITOR'S NOTE -- Burgess's North Korean Home Page address
>>is: [http://duke.usask.ca/\(tilde\)burgess/DPRK.html](http://duke.usask.ca/(tilde)burgess/DPRK.html)

⚡ Health Risk from Dusty Computer Displays

Martin Minow <minow@apple.com>

Fri, 14 Jun 1996 15:40:13 -0700

>From the electronic edition of the Swedish newspaper, Svenska Dagbladet
(14 Jun 1996) http://www.svd.se/svd/ettan/X0002_Damm_och_dator.html
(My rough translation and summary).

Workers using video display terminals in dusty and poorly cleaned offices had increased risk for skin damage, as shown by a study by the Norwegian "national work environment institute" (statens arbetsmilj=F6institut). The study showed how dust particles in combination with static electricity caused skin irritation in people working with computer displays. ...

By wiping the screens with a special ionic solution and, at the same time, grounding the hard disk, the static electricity was led away from the apparatus. The result was a noticeable lessening of skin irritation. "There were on average 20% fewer skin problems when the static electricity field disappeared," said Dr. Knut Skulberg who, together with Dr. Knut Skyberg was responsible for the project. In the control group where the ground lead was not used, there was no noticable change.

A careful analysis of the indoor environment in the offices showed how a number of additional factors were affected by static electricity. -- If there is a lot of dust, skin problems worsened. Less dust meant less skin reaction.

The researchers also discovered that few displays had strong static electricity fields directly in front of the screen. Instead, they measured the greatest values along the side and above the

displays.

Norwegian studies show that 16% of people who work frequently with computer displays have had some form of skin irritation, primarily redness, itching, and dry skin.

Martin Minow. minow@apple.com

⚡ Botched trademark search

"George C. Kaplan" <gckaplan@cea.Berkeley.EDU>

Wed, 12 Jun 1996 21:05:27 -0700 (PDT)

An article in the 12 June Wall Street Journal describes a major goof by Warner Bros. in their new movie "Eraser." In the movie, "Cyrex Corp." is the major villain, which tries to kill the character played by Arnold Schwarzenegger.

Unfortunately, the real-life "Cyrix Corp." was not amused, and threatened to sue. Warner Bros. is now busy deleting or changing all mentions of "Cyrex" in the film.

How did this happen? From the article:

So how could a major Hollywood studio make such an oversight? "It wasn't an oversight," insisted a Warner Bros. spokesman. "The names are spelled differently, and when we did a legal search it didn't show up. Sounding the same is a coincidence, that's all."

Even a rudimentary spell checker should detect that "Cyrex" and "Cyrix" are close enough to take a second look. Anyone want to

bet
that the "legal search" was nothing more than a 'grep Cyrex'?

George C. Kaplan gckaplan@cea.berkeley.edu 1-510-643-5651

✶ "Child Molester Database" on the Web

Dave Brown <dagbrown@calum.csclub.uwaterloo.ca>

Sat, 15 Jun 1996 04:39:51 -0400 (EDT)

Great World Internet Services has announced (in an off-topic posting to a newsgroup I read, incidentally) that it is keeping an on-line database of

known child molesters at <http://www.greatworld.com/public/--presumably> for

someone's information. Apart from the fact that the alleged molesters are organized by name and not by location, there is a rather alarming touch.

The site invites people to add their own molesters. What a wonderful way of anonymously slandering someone.

Great World's disclaimer states that "The responsibility for accuracy relies entirely with the persons posting the information." In other words, they come right out and say that their information cannot be trusted.

They also maintain a list of "crooked cops"--presumably also for someone's information. Given their information-gathering methods, however, both the list of crooked cops and child molesters are highly suspect, to say nothing of being serious privacy concerns.

--Dave

✶ Magellan 3000 GPS is `waterproof'?

Boyd Roberts <boyd@france3.fr>

Thu, 13 Jun 96 12:31:48 PST

I bought a Magellan 3000 GPS receiver at the weekend in London, after reading up the doc I got from the Web, and some of the reasons I bought it were because it's "rugged, durable and waterproof" and that it's housing is a "waterproof construction". Well, after it got dunked in a fountain for about 20 seconds it was no longer "waterproof", but very wet.

I suspect there's a problem with the seal around the "scratchproof" LCD display cover. Several days later, it still hasn't dried out and the construction prevents me from opening it (as does the warranty).

Risks:

As my mate Shand <shand@pa.dec.com> commented: it was better that I'd found out sooner than later and that at least I was in Trafalgar Square and I knew where I was.

Admittedly, relying on one navigation instrument is fraught with peril, but something "designed specifically for boating" is going to get wet sooner or later.

Magellan have my fax (sent yesterday), but have so far not replied.

I shall be interested in their response.

[the quoted text comes from the User Guide and the box it comes in]

Boyd Roberts
fr

boyd@france3.

⚡ Rounding errors and grammar checkers

Gabor Megyesi <G.Megyesi@pmms.cam.ac.uk>

Fri, 14 Jun 96 10:33 BST

I was reminded of the article on rounding errors on the electricity bill in [RISKS-18.17](#) when I used the grammar checker built into by MS Word, which produces statistics like average number of words per sentence after checking the text. I was surprised to see that my document had an average of 0 sentences per paragraph. On closer inspection, I noticed that the program counted 12 sentences and 17 paragraphs (do not ask me how), and must have rounded 12/17 down to 0.

This just goes to show that it is dangerous to put too much faith in anything produced by a grammar checker. My favourite is the suggestion that one should use "eye's" or "eyes'" in the sentence "The smoke makes my eyes water." The bigger risk is that someone may decide that such a grammar checker is the standard of correct English which all documents produced by the company must pass.

⚡ Re: Digital unreality

Lauren Weinstein <lauren@vortex.com>

Thu, 13 Jun 96 18:38 PDT

Jason Eisner suggests that digital cameras (at least those used for police or journalism work) be equipped with a "tamper-proof" digital signature.

There may be merit to this idea in the former case, but the concept of digital signatures in video, if applied too broadly, could have serious privacy implications, leading to concerns over making important video available for fear of retribution or similar negative consequences. Nor is it clear how much assurance could be placed in the integrity of the video itself after editing and other processing even if the original source material were "securely" tagged.

This is an area that would have to be approached very carefully and definitely not in an ad hoc manner.

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

⚡ Re: Digital unreality

Luis Fernandes <elf@mailhost.ee.ryerson.ca>

Thu, 13 Jun 1996 22:20:51 -0400

An article (AP newswire) on promotional product placement in the movies relates a story about the movie *Demolition Man* where in the North American version of the movie, Sandra Bullock's character tells Sylvester Stallone's character that only the Taco Bell franchise survived into the 2xth century.

But in versions of the movie released overseas, the franchise is changed to Pizza Hut (while both chains owned by the same parent, there are 4600 Taco Bell franchises in North America v.s. a few overseas; there are 3300 Pizza Hut franchises overseas).

"For the movie's international release, special effects experts digitally removed the Taco Bell logo from the film added a new restaurant and re-recorded Bullock's dialog. Now, when the movie is shown overseas, Taco Bell has failed... there's only Pizza Hut."

🔥 Re: Ariane-5 failures

Lauren Weinstein <lauren@vortex.com>
Thu, 13 Jun 96 18:29 PDT

David Wadsworth comments on the French commentary lagging behind events at the Ariane-5 failure. It may be remembered that exactly the same sort of lag occurred at the Challenger explosion. In both cases, the cause is probably similar. The person providing that running data commentary is typically watching a telemetry readout, not looking out a window! That displayed telemetry tends to lag events by a significant amount, accounting for the perceived effect. It is extremely unlikely that David's assumption that the "commentator" was "reading from a script" is the correct analysis in this case.

--Lauren--

✶ Physical barriers in the cockpit (RE: Damerell, F-15, [RISKS-18.20](#))

"Karl W. Reinsch" <kreinsch@radix.net>

Fri, 14 Jun 1996 00:51:44 -0400 (EDT)

David Damerell <djsd100@thor.cam.ac.uk> posted to RISKS:

>> The last low-tech solution to the prevention of triggering the missile

>> was almost comical.

I would encourage RISKS readers to check out the writings of Donald A.

Norman. Particularly relevant to this is the chapter "Coffee Cups in the

Cockpit" from `_Turn Signals Are the Facial Expressions of Automobiles_`.

Norman lists the most common and effective cognitive aids in the cockpit.

Under "crew-provided devices" he lists "written notes, coffee cups, and

tape". He specifically mentions placing an empty coffee cup over a lever as

a reminder.

I believe something similar can also be seen in the film `_Apollo 13_` with a

hard-written "Don't Touch" note placed over a switch.

-karl. kreinsch@radix.net

✶ French police raid leading ISPs

Jean-Bernard Condat <jeanbc@informix.com>

Fri, 14 Jun 1996 15:00:55 +0100

Paris, 14 June 1996--As I have so far seen no reports in the obvious Usenet newsgroups of the recent police raids on leading French Internet service-providers, and I can no longer post contributions to them myself, I send you the following English translations from the French newspaper "Liberation", which may inspire you to report them there. Note that Mr. Francois Fillon have propose one Conseil Superieur de la Telematique depending of the Bourges' CSA (Conseil Superieur de l' Audiovisuel) that will rapidly act like a high telematics authority like the new French Internet Society (ISOC).

>From the "Cahier Multimedia" of "Liberation", 3 May 1996

"Netiquette according to Mr Fillon" (La Netiquette de Fillon)

Lacking the power to police the Internet, France will invite its G7 partners (at Lyons in June) to consider the co-ordinated introduction of a "code of good conduct". A sort of "modus vivendi" which, as Francois Fillon explained to his colleagues at their recent meeting in Bologna, would guarantee a minimum degree of protection to network users. For, as the French Telecoms Minister pointed out, "if the Internet constitutes an extraordinary valuable collective resource (...), nevertheless it conceals as many risks for its users." To attempt to keep it locked up on the basis of national regulations alone would be pointless with such an inherently transnational network. Hence, according to Mr Fillon, the need

to establish
coordination at a European (OECD) level, with the aim of
drafting an
agreement [une convention]. Its signatories would establish the
principles
for legal collaboration, and a certain number of rules on ethics
and on the
legal responsibility common to on-line publishers and ISPs.
And, in the
event of a breach, the Minister also proposes to establish, once
and for
all, that "by default, the principle that the rules of the
originating
country, so far as the signatories are concerned, and [those] of
the
receiving country are applicable. "

But in "Liberation" of 8 May 1996:

"Police raid on the Internet" (Descente des gendarmes sur
l'Internet)

Two Information Service Providers (ISPs) arrested for
distributing
pornographic pictures of children, by Franck Johannes

The police are very proud of themselves, and say prudently
that "as far
as they are aware" this is a world premiere: the first time that
the police
have intervened in the Internet. Without perhaps realising what
a storm they
have produced, if not in legal circles then on the Network. The
chief
executives of two ISPs have been detained for questioning on
allegations
that they have been distributing pornographic pictures of
children.

"We keep hearing that there is a legal vacuum", explained
Lieutenant-Colonel Gerard Browne. "But that's not in fact the

case;
distributing such pictures is prohibited by Art. 227-23 of the Penal Code,
that's all". The gendarmes, who are apparently unwilling to provide
background details, were tipped-off at the end of January 1996. It seems
that a regular Net-user came across the pictures in question via FranceNet
and World-Net, both of which claim to be the leading providers of access to
the Internet. (...)

The Parisian research service immediately began exploring the services
with the support of the informatics branch of the criminal research
institute of the national gendarmerie (IRCGN). They took copies of the
various newsgroups, in other words the thousands of messages giving
information on all sorts of themes, from fly-fishing to vegetable gardening,
ultimately arriving at that with the children. This could scarcely be by
accident; it is necessary to look, for example, in a list which has the
advantage of being clear, for "alt.binary.pictures.erotic.pedophilia", to
find a prohibited picture. According to the police, some 5 to 10% of the
contents of the thousands of newsgroups accessible in this way every day are
illegal.

The dossier was transferred to the Parisian prosecuting authorities,
which in March opened an investigation entrusted to Christine Berkani, the
principal investigating magistrate in cases involving minors. On Monday [6
May] the police seized piles of floppy disks in the offices of the two ISPs,

and then the manager of WorldNet, Sebastian Sochard, and his counterpart from FranceNet, Raffi Haladjian, were arrested and held in custody on charges of "having distributed, fixed, recorded or transmitted a pornographic picture of a minor", contrary to the provisions of Art. 227-23 of the Penal Code. They risk being sentenced to up to three years in prison and fined up to half a million francs, because children under 15 years old are involved.

At WorldNet, this came as "a bolt from the blue" and his colleagues were astonished that Sebastian Socchard, 27, had been detained in custody on Monday. Last year, the young man had set up the SCT Sarl company (for Security, Concept and Technology) before becoming active as an ISP at his clients' request. Today, WorldNet has some 30 employees and claims 9000 clients, each of whom pay FF 99.00 monthly for access to the Internet.

"This affair merely illustrates the legal vacuum", protested Isabelle Perichon of WorldNet. "We don't produce any pictures, we just store them. Every day, we receive between 50,000 and 100,000 news-messages from the University at Jussieu: Jussieu sends them to France Telecom, which forwards them to us automatically." Jussieu was slightly upset by this. "France-Telecom doesn't normally get its data from us", explained an engineer from the University. "We get our news from the United States, they must be doing the same. In any case, there has never been anything like that on our server. A lot of people are anxious to prevent the network from

degenerating, and if any of them found it they would let us know within a couple of hours." The Gendarmes have plenty to keep them busy; the investigators now have to identify the source of the pictures, which "come from just about everywhere", sighed Lieutenant-Colonel Browne.

Liberation, 9 Mai 1996: "Net: si on avait su, on aurait filtre" ("If we had known, we would have filtered the Internet") - the director of WorldNet [Mr. Sebastien Socchard, an old student of the well known EPITA computer school in paris] under investigation, denies all responsibility (report by Laurent Mauriac)

In their desire to comply with French law, the ISPs are cutting off their noses in order to spite their faces. In reaction to the arrest of the managers of WorldNet and FranceNet "for simply doing their job", the four members of the French Association of Internet Professionals (AFPI) - Calvacom, FranceNet, Imaginet and Internet-way - have announced that they have cut off their subscribers' access to *all* Usenet newsgroups.

"That is the only way to apply the law", according to the director of Imaginet, Patrick Robin, who claims it would be impossible to monitor everything that is routed via his hard disks. Most ISPs carry more than 120 thousand messages every day, and any of them potentially contain pictures among which a few might be prohibited by French law.

No doubt fewer than 5% of them, according to AFPI; the whole problem is that of identifying this 5% within the great flow of continually-renewed data. That is why Patrick Robin is calling for the creation of a committee "similar to the Press's Committee for the protection of youth" and having the resources it would need to be able to inspect newsgroups regularly. The AFPI is also calling for the status of ISPs to be defined clearly: as carriers, not distributors. Making the same distinction, World-Net's director, Sebastian Socchard, commented as follows on his dealings with the law-enforcement authorities:

You could have filtered out the "outlawed" newsgroups - why didn't you do so?

[SS]: We could have removed certain newsgroups, but we didn't know which ones, or how to filter their contents. If we had know that that kind of thing was present, we would have acted.

Weren't you responsible for the distribution of the contents of everything stored on your servers?

[SS]: No, and I'm not happy with the expression "stored"; it doesn't correspond to the situation. Our equipment merely passes on pictures, it doesn't really store them. They do indeed transit via our hard disks, but that is merely part of our job of carrying them, a means to enable the users to access them more quickly. We would be equally responsible if our users obtained the pictures directly from other servers on the Web

(whereas the contents of newsgroups are stored temporarily on every ISP's server, Web pages are generally stored only on one server, and accessed directly from it when required by a user). I am not legally responsible for publishing the contents of our server.

All the same, don't you have a duty to keep an eye on the data that can be accessed through your servers? Is WorldNet responsible for everything that can be found on the Internet?

[SS]: There are 6300 newsgroups, and it would take about an hour to inspect the contents of one of them. So to check all of them in 24 hours you would need 270 people. And if we had to do that for the newsgroups, why not do it for the Web and e-mail too?

What do you think the solution is?

[SS]: I fully agree that whatever is forbidden in France ought to be filtered out, things like racism and child-pornography, for example. But it's not an easy thing to do. If one newsgroup is excluded, it can change its name or put its contents into another one. We want the government to define precisely what must be censored, as has been done for the Minitel and audiovisual services.

A lot of legal experts are saying that there is no legal vacuum; all that's needed is to apply the existing law...?

[SS]: They are assuming that the Internet is no different from other

transmission systems. In that case, we are a carrier like the rest of them, and we should be treated as such.

Do you think that you are the victim of injustice?

[SS]: If we are deemed to be responsible, then so should France Telecom or Transpac [its specialised network-operating subsidiary]. The pictures are carried through France Telecom's lines, and it is Transpac that supplies them to us automatically from its server. As the head of the Gendarmerie admitted: by attacking the two main French ISPs, they hope that the other 98 will also stop whatever they are doing wrong.

What happened when you were taken in for investigation?

[SS]: The gendarmes arrived without warning. They were well-behaved; they knew that we weren't gangsters. They said that they were simply carrying out routine procedures. It was obvious that they knew nothing about the Internet. I didn't see any experts. I suspect that the Gendarmerie wanted a high-profile operation to catch the media's attention, possibly to launch the debate. They could easily have sent us registered letters, but in that case nobody would have heard about it. Even if all this is out of all proportion for five miserable pictures, as operators we are quite happy that the debate has now begun.

Jean-bernard Condat, Senior Consultant, Smart Card Business Unit, Informix, La Grande Arche, 92044 La Defense Cedex, France +331 46963770
jeanbc@informix.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 18: Issue 22

Tuesday 18 June 1996

Contents

- [Minor real-world spelling-checker story](#)
[Mark Seecof](#)
- [About the American Hyphen Society](#)
[Bob Masson via others](#)
- [Mike's TV is kind of funny...](#)
[Michael F. O'Connor via Richard Cook](#)
- [Click *here* to lower the fuel rods](#)
[Chris Rebholz via others](#)
- [More AOL censorship \["And it reaches new lows..."\]](#)
[Barry Shein via K.Bostic](#)
- [Software products certification](#)
[Stephane Geyres](#)
- [Warning!!! Cellular Cloning](#)
[Veronica](#)
- [Re: Magellan 2000/3000 GPS nightmare](#)
[Boyd Roberts](#)
- ["Piece of Plastic" Used to Detect Drugs](#)
[Jerry Marco](#)
- [Re: "Child Molester Database" on the Web](#)
[Bear Giles](#)

[Thomas Insel](#)

● [Re: Physical barriers in the cockpit](#)

[Chiaki Ishikawa](#)

● [Some Info on Space Flight](#)

[Derek Lyons](#)

● [Re: Ariane 5](#)

[Erling Kristiansen](#)

● [Re: The European Space Agency's little problem](#)

[Prevelakis Vassilis](#)

● [Info on RISKS \(comp.risks\)](#)

✂ Minor real-world spelling-checker story

Mark Seecof <Mark.Seecof@latimes.com>

Thu, 13 Jun 1996 13:07:14 -0700

The *Los Angeles Times* recently completed a project to improve automatic spelling-checking and hyphenation for news copy (work made necessary when the paper dispensed, several years ago, with proofreaders). The automatic spelling checker previously used a both a dictionary and an algorithm that tested words against a root and a (fairly) arbitrary arrangement of common prefix and suffix strings. The algorithmic check passed many invalid words. Now it has been eliminated and only the dictionary--much expanded--is used. It took more than a month of concentrated effort to expand the dictionary to include common words previously covered by the algorithmic check. To improve dictionary-based hyphenation (the algorithmic hyphenator has also been disabled) two people spent much time over months re-hyphenating 135,000 dictionary entries. The system still makes no effort to detect

words that
are in the dictionary but that do not belong in context.

Mark Seecof

⚡ About the American Hyphen Society

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

Mon, 17 Jun 96 11:58:59 PDT

Date: Mon, 2 Oct 1995 08:35:04 -0400
>From: bostic@bsdi.com (Keith Bostic)
To: /dev/null@python.bostic.com

[>FROM: Yucks Digest Wed, 12 Jun 96 Volume 6 : Issue 6]
spaf@cs.purdue.edu (Gene "Chief Yuckster" Spafford), to
whom it was

Forwarded-by: kole@hydra.convex.com (John P. Kole)

>From: masson@convex.com (Bob Masson)

About the American Hyphen Society

The American Hyphen Society is a community-based, not-for-profit, grass-roots consciousness-raising/education-research alliance that

seeks to help effectuate the across-the-board self-empowerment of wide-ranging culture-, nationality-, ethnicity-, creed-, gender-, and sexual-orientation defined identity groups by excising all multiculturally-less-than-sensitive terminology from the English language, and replacing it with counter-hegemonic, cruelty-, gender-,

bias-, and, if necessary, content-free speech. The society's motto

is "It became necessary to destroy the language in order to save it".

Its headquarters are in Wilkes-Barre, Pennsylvania.

[Walla-Walla would do nicely for a west-coast mail-drop.

Readers who recall my 1 April 1996 excerpt from my Hyphenater's

Handbook ([RISKS-17.95](#)) may find this old item interesting.
PGN]

🔥 Mike's TV is kind of funny....

Richard Cook <ri-cook@uchicago.edu>
Mon, 17 Jun 1996 15:28:39 -0600

```
>From: mfoconno@midway.uchicago.edu
>Mime-Version: 1.0
>Date: Mon, 17 Jun 1996 06:13:33 -0600
>To: ri-cook@uchicago.edu
>Subject: Mike's TV is kind of funny....
>
>Richard,
>
>       Appreciating as I do, your preaching about the perils
of automation
>- I thought I'd forward this piece to you. Please understand
that this is
>a more understandable portrayal of your concerns than any of
your current
>examples. It would also engender substantially more political
support....
>
>>.c The Associated Press
>>
>>CHICAGO - I'll take "embarrassing mix-ups" for $1,000, Alex.
>>
>>Jeopardy viewers in 22 Chicago suburbs recently found
themselves suddenly
>>watching cavorting, naked women rather than the usual three
contestants
>>phrasing answers in the form of a question.
>>
>>About 10 minutes of the Playboy Channel was inadvertently
broadcast during
>>the time slot normally reserved for Alex Trebek's show.
>>
```

>>"Some equipment we use to cablecast was having some problems,"
Continental
>>Cablevision spokeswoman Susan Bisno said.
>>
>>She gave no details. "There's no defense," she said. "It was
awful."
>>
>>The mix-up affected scattered suburbs from Evanston just north
of Chicago to
>>Burbank, to the southwest. Continental said it will apologize
in writing to
>>customers who complain.
>>
>Michael F. O'Connor, M.D. ph: (312) 702 - 6700 DACC Univ of
Chicago

⚡ Click *here* to lower the fuel rods.

David C Lawrence <tale@UU.NET>
Mon, 17 Jun 1996 19:15:36 -0400 (EDT)

Forwarded-by: Keith Bostic <bostic@bsdi.com>
Forwarded-by: harry@sj.unisys.com
From: "Rebholz, Chris" <crebholz@sjpubs01.sj.unisys.com>

A true war story:

I used to work for the dearly departed Ingres, a relational
database
company. One day, the folks in Tech Support wandered up the
stairs to
the floor I worked on. They looked particularly ashen-faced.
Someone
finally asked them what the problem was.

Apparently, Edison Power and Light (the New Jersey equivalent of
PG&E)
had called our East Coast support office in Saddlebrook, NJ, a
half-hour
earlier. They used Ingres to keep track of the rods moving

around in the
nuclear cores on a DEC VAX. Somehow, the database had become
corrupted.
If it didn't get fixed in four hours, when the next core
rotation began,
a meltdown was likely.

Fortunately, (1) our Saddlebrook office was a half-hour from
their site,
and (2) all VAXes had the ability to have remote hardware
diagnosis
performed by their world-wide support center in Colorado
Springs, CO,
through a piece of firmware built into every VAX. Not
surprisingly, the
folks at DEC gave this problem a rather high priority. After
about an
hour and a half, it was determined that a disk sector was
corrupted. It
was repaired, and life as we continue to know it went on.

Welcome to Product Land, folks! It's got a different set of
problems than
Academia taught us all.

Remind me to tell you about answering questions about how we at
Ingres
said we would provide support during nuclear wars at a sales
call to the
Strategic Air Command some time...

🔥 More AOL censorship ["And it reaches new lows..."]

Keith Bostic <bostic@bsdi.com>
Fri, 13 Oct 1995 16:05:02 -0400

[Appeared in Yucks Digest V6 #7,
from spaf@cs.purdue.edu (Gene "Chief Yuckster" Spafford)]

From: bzs@world.std.com (Barry Shein)

So I just get a "spam" complaint from an AOL postmaster threatening:

```
>From: Postmaster@aol.com
>To: netadmin@world.std.com, postmaster@world.std.com
>Subject: Fwd: cc:Mail UUCPLINK 2.0 Undeliverable Message
>Date: Thu, 12 Oct 1995 16:49:01 -0400
```

```
> Repeated offenses of this nature will result in AOL taking
action to
> prevent further problems.
```

etc.

I look down at the message in question (they enclosed it) and it's just a few mail bounces through a mailing list out of World to some customer (look at the subject line above, some kind of cc:Mail lossage and unfortunately cc:Mail bounces back to the From: address and ignores stuff like Errors-To: and Replies-To:, constant nuisance), a list to which their customer is explicitly subscribed and apparently has been for a while.

I guess the customer didn't like the bounce message, and I guess the AOL postmaster has decided that bounce messages are "unsolicited mail". The message from the postmaster also made the point that their customers have to pay for all their e-mail so this is a problem (well, THEN *YOU* EDIT THEIR MAIL -- YOU'RE GETTING THE @\$%#^ MONEY, NOT ME!)

This is why we also have to be careful with this anti-spam crap, there are people out there, some of whom work as postmasters for the largest online services on the planet, who, are, well...you get my point, can't

quite fog a
mirror, I guess is the expression.

I took the guy off the list and told the postmaster to tell him
and tell him
that it's ok if he re-subscribes as far as I'm concerned but
perhaps that
will remind him that HE SUBSCRIBED.

Morons. I may just mass unsub all AOL addresses from all lists
here. I mean,
this is their postmaster threatening, not some random.

[I have a friend who went to work for AOL and she was
wondering why
people picked on AOL all the time. Sigh. --spaf]

[Hugh Davies <huge@axalotl.demon.co.uk> shared with me a
marvelous
list of innocent place names that would cause AOL great
grief, along the
lines discussed in [RISKS-18.07](#) and 18.08. But including the
list here
would probably cause all our AOL subscribers -- and RISKS --
to be
blacklisted. PGN]

Software products certification

Stephane Geyres <sgeyres@psti.mipnet.fr>
Tue, 18 Jun 1996 11:07:26 +0100 (WET DST)

>> A new marking for all software products <<

Software quality is a fundamental challenge in our ever changing
society, in
particular in the perspective of the use of computers and
networks by all of
us and within all sectors of social and professional life.

Fully aware of what is at stake, the AFNOR (Association Francaise de NORmalisation) General Executive Officer has just approved - in early May - the publication of the rules of a new marking called "NF Logiciel". ("Logiciel" is French for "software".) NF Logiciel is designed to be applicable to any software, whatever its application domain, its functionalities or its origin.

This adaptation of the general - and well known - NF marking is meant to be an official statement of the actual quality of those software products being marked. This marking is both an alternative and a complement to more usual quality system certification approaches:

- an alternative because it is not necessary to be certified to get the NF Logiciel marking for one's products,
- a complement because the marking requirements are based on those of quality system certification, which allows certified companies to get rather easily the NF logo for their products.

Based on sound and recognized international standards (NF ISO/CEI 12119 & ISO 9001), the NF Logiciel is an unprecedented opportunity for software providers to turn their investments in software quality into visible evidence to the end user.

Several softwares are already undergoing an evaluation and first formal markings are expected during next fall.

For more information, please contact stephane.geyres@psti.mipnet.fr

Another simple way to know much more is to send an e-mail message to our

server as follows: (Sorry, the documents are only in french so far...)

```
To: info@psti.mipnet.fr
Subject: cd nf-logiciel
send referentiel-nf-logiciel-1.0.ps
quit
```

⚡ Warning!!! Cellular Cloning

Bartle X-terminals <bartx1@library.lib.binghamton.edu>

Mon, 17 Jun 1996 15:47:17 -0400

A year ago, I brought a cellular phone in my name for a friend, due to his lack of proper documents. A month later, my first bill reflected an amount of \$1300, as a result of a fraud. I panicked and cancelled my service right away. I had to pay \$250 for early termination fee (under the contract) and an additional \$400 for my cellular phone (to keep.)

AT&T Wireless told me that they had put the case under investigation.

To make the story short, I received a letter from them (six months later,) saying that the case was not a fraud.

In the statement, more than 950 calls were made to many areas in NYC, Long Island and New Jersey. There were calls billed twice within the same time and date, made to the same number as well. Calls were made up to 14 hours in a row (, which was IMPOSSIBLE to achieve without a car) because we have a 2 hour battery. Furthermore, on the night that I had cancelled the service a year ago, my whole family, the co-user, family

friends all sat by me as I cancelled the service. I was told to document everything. Well, according to the bill, my unused cellular phone, that sat by my side, beeped a person 3 minutes before I got off the phone with the cellular representative...3 MINUTES BEFORE MY SERVICE WAS OFFICIALLY TERMINATED!!! I know for a fact that NO ONE used the phone. So who did?

This is the result of what is called cloning. AT&T refused to take my word for what happened. At this point, my case is transferred to a collective agency and it is terminated. They sent me a letter saying that there was no fraud. No signature was on the letter and the only reason given for their decision was that I had a co-user.

The moral of the story is:

1. DO NOT buy anything for anyone else, for no matter what becomes of this, I AM RESPONSIBLE for the "debt".
2. DO NOT trust cellular companies. I was told many times that this happens everyday. I was unfortunate to get such a dramatic bill. INVESTIGATION DOES NOT BRING JUSTICE. I am now left with the option to pay the money in full(with 20% off for God knows what reason,) or go to court. They warn me against it because it may cost me more...

If you have any suggestions, comments, questions or advice, please e-mail me, Veronica, at vera@gnn.com. I would appreciate it greatly.

✶ Re: Magellan 2000/3000 GPS nightmare ([RISKS-18.21](#))

Boyd Roberts <boyd@france3.fr>

Tue, 18 Jun 1996 15:46:40 GMT

After my brand new Magellan 3000 spent about 20 seconds submerged under water, causing it to fail, I bought a Magellan 2000, because I felt the need to navigate for the Housbot Escapade at the weekend.

However, the 2000 has an intermittent in it. It's some sort of mechanical problem with the receiver which causes it not to boot, switch off, reset and generally annoy you -- you have to nurse it like a baby. Faced with this, the level of confidence you place in it drops to zero -- a bad thing for a navigation instrument.

Just how easy is it to trigger this intermittent? Well, any mild shock will do; placing it on a hard surface, putting in the pocket of my CWU-36P [Jacket, Flyer's, 100% Polyamide], handing it to someone. All sorts of high-G manoeuvres like that. Fixing it requires another mild shock :-)
and some persistence with the on/off button.

You could say I'm less than happy. Where is their Quality Control?

Boyd Roberts boyd@france3.fr

⚡ "Piece of Plastic" Used to Detect Drugs

<jlm@utxvms.cc.utexas.edu>
Mon Jun 17 11:13:27 1996

>From "News of the Weird," a syndicated column, published in the Austin Chronicle on 14 June 1996:

In May, a federal judge in Beaumont, Texas, issued a permanent injunction against the Quadro Corp. of Harleyville, S.C., which had been selling a plastic box with an antenna on it to government agencies and schools for up to \$8,000 each as an illegal-drug finder. FBI tests had found the device merely a piece of plastic, utterly incapable of detecting drugs or anything else. However, several law enforcement officers and school principals swore to the judge that the Quadro Tracker worked for them.

RISKS? Where to begin? Use of a device without any knowledge of its workings. Believing anything the sales guy tells you. Failure to run controlled tests on a device before placing it into service. Believing that a box with an antenna on it could possibly detect drugs in the first place. Hiring credulous individuals as "police officers and school principals." Placing near-dictatorial power in the hands of school principals.

Perhaps someone else has more detail. I'm particularly interested in the assertion that the Quadro Tracker "worked for them," and in the fate of those whose supposed possession of illegal drugs was detected by the device. Were the individuals searched? Are those searches now deemed to have been illegal? Was action taken against anyone on the grounds of the Quadro Tracker's results alone? On what basis do the officials believe that the Quadro Tracker worked?

[PGN, I'll preemptively note that the judge made the "illegal-drug finder" an "illegal drug-finder."]

Jerry Marco University of Texas General Libraries jlm@utxvms.
cc.utexas.edu

✶ Re: "Child Molester Database" on the Web (Brown, [RISKS-18.21](#))

Bear Giles <bear@indra.com>

Mon, 17 Jun 1996 22:05:48 -0600 (MDT)

The official registries maintained by states (which can hurt you in much more serious ways than a web site) use information sources which are just as questionable.

As I recall, in Colorado therapists are required to report the name of any patient reporting being a victim of sexual child abuse, if the individual is 27 or younger. This stellar example of legislative reasoning was based on the observation that many (most?) abusers were themselves abused. Therefore "anyone who was a victim is likely to be an abuser and should be tracked." The cutoff age was apparently based on another statistic with equally dubious pedigree.

This might not be so bad if the registry was well run, but it appears (from the discussions in the local media) that once you're on the list there's no distinction between people actually convicted of crimes and people who were listed due to nasty divorce battles or therapy sessions. Furthermore, it's virtually impossible to remove your name from the list once it

has been
added. Cries of innocence are viewed with the same skepticism
as we hear in
the cryptology debate -- if you have nothing to hide, why are
you so
bothered?

✉ Re: "Child Molester Database" on the Web (Brown, [RISKS-18.21](#))

Thomas Insel <tinsel@jaka.ece.uiuc.edu>

Tue, 18 Jun 1996 05:47:42 -0500

> ... In other words, they come right out and
> say that their information cannot be trusted.

Worse still, the author realizes the possibility that listed
people
may be upset and reports recent experience with false listings.
Nevertheless, according to the dispute resolution procedures at
<http://www.greatworld.com/public/mdispute.htm>
the only authentication required from an accuser is a valid e-
mail address,
and if the poster claims to be a victim, relative of a victim,
or friend of
a victim, a disputed listing will stand, even without a
conviction. He
claims that a posted rebuttal will provide "more than equal
opportunity" for
defense.

I'm not a lawyer, but surely these policies leave the listings'
proprietor
open to an incredible (and probably justified) libel suit,
during which it
may be impossible to identify the original accuser.

Tom

✈ Re: Physical barriers in the cockpit (Re: Reinsch, [RISKS-18.21](#))

Chiaki Ishikawa <ishikawa@personal-media.co.jp>

Tue, 18 Jun 1996 21:30:29 +0900 (JST)

I admit that placing plastic cap, or even a paper coffee cup(?) is a great way to remind pilots not to touch certain levers and/or buttons. I often do something similar if I want nobody to touch certain computer keyboard while some important tests are under way on the machine.

What bothered me in the shooting down of F-15 and its subsequent investigation is that the investigation team didn't go down to the bottom of the real cause of why the main firing system became active despite the main switch being turned off. Static electricity was rumored to be the cause initially, but in the final report, as far as I read in newspaper articles, no clear culprit was mentioned.

This means that there might be, albeit with very small possibility given that F-15s have been flying in the sky all over the world for so many years, a rare bug such that the firing system may spontaneously fire missiles no matter what the main switch position is and whether trigger button is pressed or not. (Am I getting paranoia these days?)

Placing a plastic cap may be useless if such rare (still possible) bug lurks in the system, and I felt disappointed that the investigation team let the bug go unnailed. It would indeed be comical if a poor pilot finds one day a

missile is launched while the plastic cap is firmly in place...
Well, not so
comical, come to think of it.

BTW, I am eagerly waiting for the initial words regarding the
cause of
shooting down of American plane by a Japanese navy boat.

Chiaki Ishikawa Personal Media Corp. Shinagawa, Tokyo,
Japan 142
ishikawa@personal-media.co.jp

⚡ Some Info on Space Flight

Derek Lyons <elde@hurricane.net>
Mon, 17 Jun 1996 12:59:27 -0700

Some serious misconceptions here, pardon me while I clear them
up.

>From: frank@artcom.de (Frank Rieger, [RISKS-18.19](#))
>Subject: Matra made software for Ariane5 AND Taipei subway
system ([R 18.17](#))

>On the base of the information available now, I ask myself, why
was there no
>mechanism to avoid the control computers' attempt to go into
this extreme
>flight position?

Why would you want to? The Control Computers *job* is to
control the
position of the engines. Redundant hard/software to correct for
possible
errors in the primary computers costs horribly in terms of
weight and
reliability, as well as being difficult to engineer and test.
In addition
is is extremely unlikely that a redundant system would detect a

software
glitch in time to prevent such a failure.

Study the STS/Orbiter flight control systems for an object lesson in this.

>Date: 10 Jun 1996 11:17:05 -0400
>From: "James Brady" <jlbc@eci-esyst.com> ([RISKS-18.19](#))
>Subject: Re: The European Space Agency's little problem (Wood, [RISKS-18.18](#))

>
>(The Space Shuttle can actually abort during launch under ...)

No, the SRB's cannot be separated while burning. The stresses would tear the whole stack apart. (Uncontrolled separation (the only kind available at that point in flight) is what caused the Challenger to break up.)

All STS abort modes require that the SRB's be ridden to burnout, and the that ET be nearly empty prior jettisoning it.

>Date: Sat, 08 Jun 1996 21:31:59 EDT
>From: Marc Horowitz <marc@MIT.EDU> ([RISKS-18.19](#))
>Subject: Re: The European Space Agency's little problem (Wood, [RISKS-18.18](#))

>
>Apollo carried more valuable cargo than any commercial rocket. Remember, it >was the apollo astronauts who forced NASA to design a window into the >capsule, at a very high cost.

This objection could only possibly be applied to the Mercury program, as a window was required for the objectives of both the Gemini and Apollo programs.

In addition, the window proved its worth again and again during the Mercury program as any cursory study of the flights will show.

✶ Re: Ariane 5

Erling Kristiansen <erling@wm.estec.esa.nl>
Tue, 18 Jun 1996 09:37:21 +0200 (MET DST)

Excerpt from ESA press release 22-96:

- > FLIGHT 501 FAILURE - VEHICLE EQUIPMENT BAY RECOVERED

- > Investigation of the flight 501 failure has been under way
- > since 4 June. In particular, a large part of the equipment
- > contained in the vehicle equipment bay has been recovered
- > and inspected. This has revealed the existence of a
- > malfunction
- > relating to the inertial platforms in Ariane-5 operating mode.

Erling Kristiansen (erling@wm.estec.esa.nl)
European Space Research and Technology Centre (ESTEC)

✶ Re: The European Space Agency's little problem (Brady, [RISKS-18.19](#))

Prevelakis Vassilis <vp@cui.unige.ch>
Tue, 11 Jun 1996 12:59:41 +0200

- > [...] (The Space Shuttle can actually abort during launch
- > under
- > specific conditions and return to the landing strip at
- > Kennedy, or go on to
- > a down-range site, or ditch in the ocean. Had sensors been
- > available to
- > tell the crew or ground controllers of the burn-through
- > problem, one of
- > these abort modes might have been employed with the chance of
- > saving the
- > crew if not the vehicle.)

There are two errors in the above paragraph. The first concerns the ditching into the Atlantic. It has been said again and again that the Shuttle does NOT have the ability to ditch into the ocean. The airframe is not sturdy enough to withstand the impact and the external surface (mostly made of fragile tiles) will disintegrate.

It is true that in the pre-Challenger era if the astronauts found themselves in a position where ditching was the only alternative they were doomed. Nowadays they will be able to bail out using the extensible pole and parachutes while the Shuttle is kept on a level flight.

The second error concerns the survivability of the Challenger failure. There was and there is no way to detach the Shuttle from the external tank while the SRBs are firing. So abandoning the failing external tank was not an option. What can be argued is that since the astronauts were not rendered unconscious from the violent separation, if they were wearing pressure suits instead of air packs they might be able to find their way out of the cabin and bail out. While this cannot be ruled out it is unlikely because the inside of the shuttle cabin is not exactly spacious and it must have been tumbling. Next, at this stage we are not talking about the shuttle, but about a part of the shuttle with bits hanging from it, no power and no way to keep it stable. If the pilots had ejector seats (like they had for the first test flights back in the early eighties) they could try ejecting, but

I just can imagine the Challenger crew finding their way out in time to avoid the crash.

=====

Now about the Ariane discussion. If the payload is irreplaceable, you don't send it aboard the first test flight of a new rocket. You pay for a normal flight which is also insurable (assuming the test flights are successful). Insurance in the satellite business is a hedging of the risk. If an operational launcher blows up then the premiums paid for all subsequent launches go up so that insurers can recoup their costs. So the launch clients collectively pay for the failure anyway. Insuring is thus a way to evenly spread the cost of failure.

Remember that the Ariane failure mode is not that common. In most cases it is upper stages that fail, the satellites get placed in the wrong orbit or simply disappear. Parachutes will not save them in these cases. Also a launch vehicle will either evolve to be unlikely to blow up during launch or it will not be used. So putting parachutes will guard against an event that will have a steadily decreasing probability of occurrence. So we have to argue that we should put the ejection mechanism only on the first few flights (the Shuttle approach). In this case we have to balance the cost of developing the escape system against the cost of the cargo that will be saved IF the launcher fails. To this we have to add the cost of the replacement launcher and the cost of refurbishing the cargo

after its
recovery and preparing it for the next launch. You don't just
pick it up and
stick it back into the next Ariane.

Now the developers of the first Ariane 5 payload didn't have
enough money
for buying space on a commercial launcher, so they wouldn't have
money for
the escape system anyway. Maybe the falacy of the whole
situation is that
they were allowed to spend \$500 million without budgeting the
\$65 million
launch costs.

Vassilis Prevelakis CUI University of Geneva



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 18: Issue 23

Monday 24 June 1996

Contents

- [The Great Netcom Crash.....](#)
[David Lesher](#)
- [Microsoft, AOL, and AT&T also have netwoes](#)
[PGN](#)
- [Subject: Pachinko in the armor?](#)
[PGN](#)
- [DoD and IRS tax systems](#)
[Richard L. Wexelblat](#)
- [Unexpected risks of usability features](#)
[Steve Loughran](#)
- [Espionage Suit](#)
[David Kennedy](#)
- [Pointless PINs](#)
[Mark Seecof](#)
- [Re: Click *here* to lower the fuel rods](#)
[Nancy Leveson](#)
- [Urban Legends?](#)
[William Petrick](#)
[Charles Waite](#)
- [Re: More AOL censorship](#)

[Edward Reid](#)

[Ray Everett-Church via Mike Epstein](#)

● [Re: Spelling-checker war stories](#)

[Andrew Koenig](#)

[Kevin Haw](#)

● [Static, dust, and other risks](#)

[Rob Slade](#)

● [Re: Health Risk from Dusty Computer Displays](#)

[Terje Mathisen](#)

● [Re: "Piece of Plastic" Used to Detect Drugs](#)

[Douglas W. Jones](#)

● [Info on RISKS \(comp.risks\)](#)

⚡ The Great Netcom Crash.....

David Lesher <wb8foz@netcom.com>

Fri, 21 Jun 1996 12:45:56 -0400 (EDT)

Netcom, Inc; one of the largest retail ISP's [450,000 subscribers, 230 POPs] went down for 14+ hours this week.

In what strikes me as "shades of Mariner II" Netcom President David Garrison, appearing on KGO Radio said it was an extra "&" in the "border gateway protocol code" in the MAE-East router in DC area that killed the system.

They had to bring down all 100+ routers & flush each one to recover, he reported.

The parallel to the Bell Atlantic STP bug of about five years back strikes me. The routing nut has gotten so tough that the tools used on it can be [VERY!] rapidly fatal.

⚡ Microsoft, AOL, and AT&T also have netwoes

<"Peter G. Neumann" (Neumann@CSL.sri.com)>>

Mon, 24 Jun 1996 12:03:17

An article by Peter H. Lewis in **The New York Times**, 24 Jun 1996, p. D1, noted the Netcom problem ("for 12 hours") noted in [RISKS-18.23](#) by David Leshner. The article also noted these other problems:

- * Microsoft shut down its nationwide network on Sunday (presumably 23 Jun 1996) for 10 hours as part of an intended backup power-supply upgrade, but the upgrade failed and they will have to try again.

- * America Online was out of service for an hour on 19 June "1996, when a planned system software upgrade backfired."

- * AT&T will shut down its Internet access for up to 8 hours each week, for maintenance.

⚡ Pachinko in the armor?

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

Thu, 20 Jun 1996 08:34:39 -0800

There was a nice article surveying the pachinko bogus-card fiasco noted in [RISKS-18.15](#) and 16, and the risks of believing in technological solutions to

not-just-technological problems.

Printed-version title:

Counterfeiters of a New Stripe Give Japan One More Worry;
Fake Cards Thwart Efforts to End Pinball Scams
By ANDREW POLLACK, *The New York Times*, 20 Jun 1996, D1

On-line-version title:

A Case Study of the Hazards of Electronic Cash
By ANDREW POLLACK, c.1996 N.Y. Times News Service, 20 Jun 1996

[Text seemingly identical in both versions.]

⚡ DoD and IRS tax systems

"Richard L. Wexelblat" <rwex@CLARK.NET>

Thu, 20 Jun 1996 21:38:14 -0400

Special note: I work for the IRS and have a work-related vested interest

===== in not having the Department of Defense involved in

contracting for IRS software and systems.

Therefore,

despite any claims of non-bias below, I am clearly "interested" in the classical sense of the word.

That part out of the way, I'd like to say (as a private citizen, a tax-and-spend liberal, and an almost-always defender of free speech and the right of the citizen to privacy) that the present initiative by Congress to have DoD become the contracting agent for IRS system and software development is a clear and present danger to privacy in the Republic in which we stand.

The initiative referred to above is in the "Subcommittee Mark"

of the proposed next year's budget. It's just a House Subcommittee so it's not law, but it's a bad idea in my mind, even to consider it seriously. Is the Department of Star Wars and the \$700 toilet seat really so excellent a contracting agency that they are the clear choice to handle IRS business?

Well, that's my biased opinion, and I'd like very much to hear from others who may have a more valid claim to disinterest!

Dick Wexelblat, Acting Lead Architect << asa APbA IRS

⚡ Unexpected risks of usability features

Steve Loughran <slo@HPLB.HPL.HP.COM>

Thu, 20 Jun 96 13:50:22 BST

An entertaining part of Windows 95 is the time-zone chooser in its control panel. As well as being able to select time zones like (GMT +01:00), users who don't know or care about their meridan-relative time zone can just click on a map of the world. The appropriate time zone is then highlighted and -the cute bit- the whole world smooth scrolls round so that the user's country is in the centre of the map.

In the latest beta of Windows NT 4.0, the map is still there but is disabled: no mouse clicks are responded to and no highlights appear. The smooth scrolling still works, but with timezone selection via a list it is nowhere near as cute as it used to be.

What is interesting is the reason it doesn't work. It is not, as one would expect, a technical problem, but a political one -and thus a lot harder to fix:

>From "Windows NT 4.0 Beta 2 Commonly Reported Problems",
Version 3.0
June 15th, 1996:

> 3.7.1: Time zone map does not respond to mouse and display highlight

> Status: Due to international border disputes we have removed this

> functionality There are numerous timezones that follow international

> borders that are not universally agreed upon. In order to satisfy all

> parties involved in these disputed areas we chose not to display any

> borders at all. We are aware it is a feature that many people miss.

✶ Espionage Suit

David Kennedy <76702.3557@CompuServe.COM>
{[lost.] *somewhen recent*}

Courtesy of Associated Press via CompuServe's Executive News Service,
19 Jun 1996

Espionage Suit

By ANTHONY JEWELL, Associated Press Writer

>> INDIANAPOLIS (AP) -- Johnson & Johnson's diabetes products
>>subsidiary encouraged workers to illegally spy on rivals and

>>gave "Inspector Clouseau" and "Columbo" awards for those who
>>got the most information, a competitor charged Wednesday.
>> Boehringer Mannheim Corp., a German-owned drug and medical
>>device company, made the allegations in a federal court lawsuit
>>against J&J and its LifeScan Inc. subsidiary. Boehringer has
>>U.S. offices in Indianapolis. [...]

- o Suit asks for Lifespan to cease using Boehringer's trade secrets and seeks unspecified damages.

- o J&J says both companies did it but its LifeScan received no competitive advantage from their activities.

- o Suit alleges that LifeScan used third parties as well as their own employees to collect information about Boehringer. And that LifeScan "infiltrated" private meetings at Boehringer.

- o A former LifeScan employee broke the news in May 94.

>> Boehringer's lawsuit said two LifeScan employees
>>"deliberately fostered an environment which made clandestine
>>and illegal activities directed at competitors ... both routine
>>and expected."

>> Mannheim said David Van Avermaete and Daphne Flamer
>>initiated the "Inspector Clouseau Award," the "Columbo Award,"
>>and the "Mrs. Fletcher Award," after the lead character in the
>>TV series "Murder, She Wrote."

>> The awards were allegedly "presented at meetings, with
>>prizes, to members of the sales force who obtained the best
>>information about competitors and their plans," the lawsuit
>>said. [...]

>> The suit claims a LifeScan employee stole a prototype of a
>>diabetes monitoring system known as Accutrend DM. Oldham said
>>the prototype was stolen in Europe, taken to a LifeScan
>>California lab and returned to Europe. [...]

>> Boehringer Mannheim, which had 1995 sales of more than \$700
>>million, employs more than 3,500 people at facilities in

>>Fremont and Concord, Calif., and Gaithersburg, Md.

Dave Kennedy [CISSP] InfoSec Recon Team Chief, National Computer Security Assoc

Pointless PINs

Mark Seecof <Mark.Seecof@latimes.com>

Tue, 18 Jun 1996 15:03:05 -0700

A colleague just got a handheld cellular telephone. The device asks the user to enter a 4-digit PIN before it will permit outbound calling. The vendor (local cell-phone duopoly carrier, not an independent) has set the PIN to the last four digits of the assigned telephone number, which the phone displays upon powerup BEFORE asking for the PIN. This helps people with poor memories and people with no authority equally. The vendor's service staff state that they have a fixed policy of configuring all 'phones this way. A longer (5 or 6 digit) "security code" enables users to change the PIN, but the vendor refuses to supply that code to my colleague (presumably to retard his ability to switch carriers for which that code is also needed). The vendor will allow my colleague to bring the 'phone to an inconvenient location during limited hours at his own expense to have the PIN changed; if he does this he must tell his PIN to the vendor's staff (they already have the "security code," but he would be revealing his PIN-choosing habits). My colleague wonders why the phone has a PIN if it

offers zero security!

⚡ Re: Click *here* to lower the fuel rods (Rebholz, [RISKS-18.22](#))

Nancy Leveson <leveson@cs.washington.edu>

Tue, 18 Jun 1996 21:12:15 PDT

>Somehow, the database had become corrupted. If it didn't get fixed in

>four hours, when the next core rotation began, a meltdown was likely.

This didn't make any sense to me from what I know about nuclear power plants so I checked with a friend who is an engineer at one of the U.S. nuclear power plants. It's hard to reconstruct what really might have been the case. The computer could have been computing control rod movements and printing them out for an operator to use to manually control the rods (this is not done automatically) and there might have been no contingency plan or the operators might not have been able to do the computation manually in the time required. Could that have caused a meltdown? No. At worst, it might have required the operator to reduce power or to shut down the reactor.

⚡ Urban Legends? (Fuel Rods, Rebholz, [RISKS-18.22](#))

William Petrick <caprit@ix.netcom.com>

Wed, 19 Jun 1996 09:27:30 -0700

> "A true war story:"

Just because someone says it, and others forward it does not make it true.

This must be an attempt to establish a new urban legend. There are enough misconceptions about commercial nuclear power plants already, so we need to avoid creating fantasies that can be made into exciting movies.

First, there is no Edison Power and Light. The two utilities operating nuclear plants in New Jersey are Public Service Electric and Gas (PSE&G) and GPU Nuclear Corp., operating plants in Salem NJ and Forked River NJ, respectively. There is also Consolidated Edison of NY, which runs a nuclear plant in Buchanan, NY.

Second, rods do not move around in a nuclear core and there is no next core rotation.

Third, Ingres and DEC VAXes are not used in safety systems in nuclear power plants, so neither could have any impact on whether a meltdown was likely.

> Remind me to tell you about answering questions about how we at Ingres
> said we would provide support during nuclear wars at a sales call to
> the Strategic Air Command some time...

Another urban legend?...

My best guess is one of two possibilities:

(1) One of these plants was shut down for refueling, during which time they remove spent fuel bundles and replace them with fresh fuel. During this

process, they also move (rotate?) other bundles to new locations for the next year of operation. The offline computers are used to maintain records of the location of each bundle throughout its life in the core. If that database gets corrupted, the utility must revert to tracking everything by hand -- a laborious and time-consuming process. The four-hour window could have been because the refueling is a critical-path item during an outage and delays can cost millions of dollars in lost revenue.

(2) One of these plants was planning a control rod sequence exchange to maintain a uniform fuel burnout throughout the core. These rod patterns are precalculated in DEC VAX computers and may involve an Ingres database. Sometimes these exchanges are done at reduced power, so the four hour time limit may have been the time at which they had to be back at full power or they might have to shut down, again an economic decision that involves millions of dollars.

In either case, there is no safety issue.

In fact, there are very few commercial nuclear plants in the US that use computers or software in any safety system. Upgrades to safety systems that include digital technology is an ongoing area of development between the industry, research groups, and the regulatory agency (Nuclear Regulatory Commission). There are also safety-critical discussion groups on the Internet that exchange ideas. Because of misconceptions of how safety systems are defined and used in nuclear plants, I published a

WEB page for
the safety-critical group that may help understand the context
of safety in
nuclear power applications. Anyone who posts nuclear power
plant examples
should review that article at: [http://www.netcom.com/~caprit/
ctisafet.html](http://www.netcom.com/~caprit/ctisafet.html).

The risk of this article is the rapid spread of misinformation!

✶ Urban Legends? (Fuel Rods, Rebholz, [RISKS-18.22](#))

Charles Waite <waite@waterw.com>

Thu, 20 Jun 1996 20:07:55 -0400

I love war stories, but alas, the story from: "Rebholz, Chris"
<crebholz@sjpubs01.sj.unisys.com>, is not true.

As a resident of New Jersey, I am unaware of any Edison Power
and Light.

There are also four nuclear power plants in New Jersey, and I
have worked at
all four, in groups responsible for the process computers.

>A true war story:

As the former Principal Engineer for Digital Systems at PSE&G's
(California's equivalent of PG&E) three nuclear plants, I assure
you there

are no computer moving control rods. There are computers used
to compute

rod worth for future fuel loads, but no nuclear plant in this
country

entrusts computers to move rods in such a way as to cause a
meltdown. Most

of the rod moving components and systems are old analog
systems. The

closest a computer comes to actual fuel movement is through a
computer - a

"rod-worth minimizer" - that will stop an operator from pulling control rods out of the prescribed, analyzed, approved "pull sheet."

The real problems with computers at nuclear plants are actually much more interesting. I'll submit an example I posted in another group a few months ago if I can find it on my archive tape. But for now, let's get real.

Charles Waite, Kemper-Masterson, Inc., c/o 38 Fox Run
Mount Laurel, NJ 08054 (609)235-4275

✉ Re: More AOL censorship (Bostic, [RISKS 18.22](#))

Edward Reid <ed@titipu.resun.com>

Thu, 20 Jun 96 10:29:18 -0400

A lot of people beat up on AOL for good reasons. At least as many beat up on AOL without knowing what they are talking about. I have no love for AOL, but I see no reason to attack them for things they didn't do.

> >From: Postmaster@aol.com

This is suspicious to start with. I've corresponded with AOL admins on numerous occasions, including David O'Donnell, who normally acts as AOL postmaster. I've never received a message indicating it was from postmaster@aol.com. The admins all use their individual e-mail addresses. In fact, AOL actively discourages e-mail to postmaster because it delays the response while someone sifts through the volume of e-mail to forward it to the responsible individual within AOL. They provide other

addresses for
reporting abuse, etc.

> message from the postmaster also made the point that their
customers have to
> pay for all their e-mail so this is a problem (well, THEN
YOU EDIT THEIR
> MAIL -- YOU'RE GETTING THE @\$%#^ MONEY, NOT ME!)

This clinches it. AOL customers do not pay to receive e-mail and
never
have. Many people make this mistake; it was Compuserve that once
charged to receive e-mail. The AOL postmaster would of course
know this,
so the message is a clear and unmistakable forgery.

I suggest that the original recipient examine the message
headers more
closely. Someone who can't even get the basic facts about AOL
right
probably didn't forge the headers very well either.

> This is why we also have to be careful with this anti-spam
crap, there are
> people out there, some of whom work as postmasters for the
largest online
> services on the planet, who, are, well...you get my point,
can't quite fog a
> mirror, I guess is the expression.

Yes, world.std.com is a large online service and someone who
works
there can't detect an e-mail forgery ... well, you get my point.

> Morons. I may just mass unsub all AOL addresses from all lists
here. I mean,
> this is their postmaster threatening, not some random.

On the contrary, it *is* some random.

On the other hand, the posting to comp.risks didn't show the full
headers of the message from bzs@world.std.com, so maybe that was
a

forgery too. Not to mention that I have no way of knowing whether bzs actually works for world.std.com. I hope not; this posting is so rude that I hate to attribute it to anyone working for any service provider.

Edward Reid <reide@freenet.tlh.fl.us>

✶ Re: More AOL censorship ([RISKS-18.22](#))

Mike Epstein <epstein@nyiq.net>

Thu, 20 Jun 96 11:45:07 -0400

This was posted on SPAM-L, a list devoted to ending spam, by an AOL Assistant Postmaster. He gave his permission for me to send it to you.

Date: Wed, 19 Jun 1996 23:12:09 -0400
>From: Ray Everett-Church <IFRITRay@AOL.COM>
Subject: Re: Interesting AOL message

>From: bzs@world.std.com (Barry Shein)
>So I just get a "spam" complaint from an AOL postmaster threatening:
>>From: Postmaster@aol.com
>>To: netadmin@world.std.com, postmaster@world.std.com
>>Subject: Fwd: cc:Mail UUCPLINK 2.0 Undeliverable Message
>>Date: Thu, 12 Oct 1995 16:49:01 -0400
>> Repeated offenses of this nature will result in AOL taking action to
>> prevent further problems.

I'd be **most** interested in seeing the ENTIRE original message from AOL.

I'm quite surprised to see mail bouncing off a server being called

"SPAM"...unless it's a junk mail list (replies to the junk

mailers
usually bounce as a normal course of events).

In full disclosure, some time last month I had an e-mail conversation with Mr Shein that ultimately ended in a stream of obscenities from him. We were talking about the fact that "world.std.com" gives a home to DEMC, a major junk mail outfit. They spam from throw-away accounts at ISPs, but point replies back to their autoresponder firmly ensconced at DEMC.COM, which is served by world.std.com. I sought to explain that by providing a stable return address, he is aiding DEMC in its spamming activities.

[Strong response omitted. PGN]

Ray Everett-Church, Asst. Postmaster (everett@aol.net,
IFRITRay@aol.com)
America Online's Internet Development Outreach and Technology
Team
<http://www.everett.org/~everett> AOLers misbehaving? mail:
abuse@aol.com

✉ Re: Spelling-checker war stories

Andrew Koenig <ark@research.att.com>
Thu, 20 Jun 1996 08:32:37 +0400

In [RISKS-18.22](#), Mark Seecof notes that spelling checkers that use prefix and suffix tables can find nonwords. I saw a paper by Doug McIlroy a number of years ago that noted two such nonwords that have a good chance of appearing in actual documents: thier and presenation.

After all, if you can derive flier from fly, you can derive thier from thy.

And if you can derive relation from relate, you can derive senation from senate, hence presenation.

Incidentally, Doug noted that the most frequently misspelled word in his sample was `accommodate,' which he found seven ways to misspell.

Andrew Koenig ark@research.att.com

⚡ Re: Spelling-checker war stories

Kevin Haw <haw@ecs.fullerton.edu>
Sat, 22 Jun 1996 21:55:41 -0700 (PDT)

A few years ago, an author in the UK's PUNCH shared the most interesting phrases that made it past his spellchecker, but were caught by his editor.
My personal favorite: a reference to the Prime Minister "Margret Hatchet".

- Kevin N. Haw haw@titan.ecs.fullerton.edu

⚡ Static, dust, and other risks (Minow, [RISKS-18.21](#))

"Rob Slade" <roberts@mukluk.hq.decus.ca>
Tue, 18 Jun 1996 16:19:07 EST

Martin's posting reminded me of something I found while researching health risks associated with computers some time ago. Please bear with me: the original article was not a formal review of the study, and I

haven't got a
reference for it.

Going strictly from memory, this involved an Australian company. The data entry/query clerks, almost universally, were suffering from facial skin rashes and attributed it to radiation from the monitors. A physician, consulted about the problem, prescribed a barrier cream, and the skin rashes disappeared.

Someone knew enough about physics to note that 1) monitors don't produce that much radiation and 2) barrier creams wouldn't stop radiation anyway. An investigation was launched into the real cause.

The work of the department involved looking up long columns of numbers. The workers were in the habit of running their fingers down the screen in order to pinpoint the item they needed. Static attracted dust, make-up, and other pollutants to the screen, and the fingers transferred these to the workers' faces. Hence the rash.

The barrier cream provided some protection against the pollutants. More than that, however, it was greasy. Workers who ran their fingers down the screens found they were making streaks on the monitor. Therefore, they learned not to touch the screen--and no longer picked up pollutants.

✉ Re: Health Risk from Dusty Computer Displays (Minow, [RISKS-18.21](#))

Terje Mathisen <Terje.Mathisen@hda.hydro.com>

Mon, 24 Jun 1996 12:08:15 +0200

I took part in this study, and got some interesting information from the guy from the Physics Department of Oslo University who did the field measurements on my machines:

With modern low-emission crt displays, i.e. like the Nokia 21" MultiGraph 445X screens in my office, the keyboard can (and did, in my case) radiate more than the crt! The crt was the predominant source of static electricity, however.

The computer enclosure as well as crt and keyboard was grounded, not the hard disk.

- <Terje.Mathisen@hda.hydro.com>

⚡ Re: "Piece of Plastic" Used to Detect Drugs (Marco, [RISKS-18.22](#))

Douglas W. Jones <jones@pyrite.cs.uiowa.edu>

18 Jun 1996 17:12:25 GMT

KCRG, A local TV station in Cedar Rapids went into some detail on the story because the local school district almost bought the widget, and another local district did, and was satisfied with what they got.

The Tracker had an empty plastic "electronics box" you wore over your shoulder, connected by a coiled telephone-style cord to a pistol grip. The antenna was hinged to the pistol grip so it could swing very

freely from
side to side, and the operating instructions were to hold the
grip so that
the axis of the hinge was exactly vertical.

As a result, like a classic dousing rod, very slight
subconscious hand
movements can cause wild changes in where the antenna points.
The result,
in the hands of a skilled practitioner can be as gratifyingly
accurate as a
dousing rod, but of course, what it's doing is uncovering
subconscious
guesses on the part of the practitioner, not pointing at water
or drugs.

Perhaps I should start selling forked birch sticks to police
departments?

Doug Jones jones@cs.uiowa.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 18: Issue 24

Tuesday 2 July 1996

Contents

- [Workmen strike at CERN](#)
[Al Smith](#)
- [Ariane 5 Crash due to Faulty Software?](#)
[Andy Fuller](#)
- [c4i-pro The Millennium comes early to GPS](#)
[Joe Gwinn via Tom Briggum ...](#)
- [Police Computer Stolen](#)
[David Kennedy](#)
- [Automatically generated typos in online Sydney Morning Herald](#)
[Tom McDermott](#)
- [Grammar checkers](#)
[John Colville](#)
- [The computer is always right - again](#)
[Hugh J.E. Davies](#)
- [Metro Machiniste leaves train for coffee](#)
[Boyd Roberts](#)
- [Blackmailing financial institutes - a real life story](#)
[Frank Rieger](#)
- [Re: DoD and IRS tax systems](#)
[Dennis G. Rears](#)

[Scott A. Renner](#)

[Carl Minie](#)

● [Digital Precipice: What the computer trade hides from their customers](#)

[Kirsten Raach on Markus Gaulke's book](#)

● [Info on RISKS \(comp.risks\)](#)

✂ **Workmen strike at CERN**

Al Smith <Al.Smith@gold.net>

Wed, 26 Jun 1996 15:19:59 +0200

After a shutdown of 6 months during which the LEP vacuum system was opened at many locations, the accelerator was started up on 14 June 1996.

After 5 days of machine studies it became clear that there was an obstacle inside the LEP vacuum chamber close to Point 1. On the morning of 19 June the vacuum system was opened and 2 empty beer bottles, some 5 metres apart, were found inside the beam pipe. This incident has caused a 5 day delay in the setting up of the accelerator and will result in a reduction of about 10% of the time available for running LEP2 at the W pair production threshold (161 GeV) in 1996.

✂ **Ariane 5 Crash due to Faulty Software?**

Andy Fuller <acfa@eci-esyst.com>

Fri, 28 Jun 1996 09:11:45 -0400

According to the 24-30 June issue of *Space News* the 4 June

1996 explosion of the Ariane 5 rocket was caused by software in the inertial guidance system. Apparently an inertial platform from the Ariane 4 was used aboard the Ariane 5 without proper testing. When subjected to the higher accelerations produced by the Ariane 5 booster, the software (calibrated for an Ariane 4) ordered an "abrupt turn 30 seconds after liftoff", causing the airframe to fail.

The article notes that a request to test the inertial platform under conditions similar to those produced by the Ariane 5 was "vetoed by CNES for budgetary reasons." Sextant Avionique, the builder of the inertial platform, has since performed these tests and confirmed that it would fail in an Ariane 5 launch.

We are again reminded that crashing a simulator is lots cheaper than crashing a vehicle.

Andrew C. Fuller Raytheon E-Systems | Box 12248 | St.
Petersburg, FL 33733
acfa@eci-esyst.com (813)381-2000 x3194 | Fax:(813)381-3329

c4i-pro The Millennium comes early to GPS

<>

Thu, 27 Jun 1996 09:36 -0500 (EST)

[Via Bruce_Walter@ccmail.orl.mmc.com and
Bob Schaefer <schaefer@rapnet.sanders.lockheed.com>]

"tom briggum" <tom_briggum@ccmail.nctamslant.navy.mil>

Don't know the validity of the following, but it sounds authentic

to me. Talk about your major C4I problem!

... Tom Briggum

>From: gwinn[SMTP:gwinn@ed.ray.com]

Sent: Wednesday, June 26, 1996 11:48 AM To: osswgx

Subject: The Millennium comes early to GPS

I have good news and I have bad news.

The good news is that GPS will not have a "Year 2000" problem.

The bad news is that GPS System Time will roll over at midnight

21-22 August 1999, 132 days before the turn of the millennium.

On 22 August 1999, unless repaired, many or all GPS receivers

will claim that it is 6 January 1980, 23 August will become 7

January, and so on. I would expect that some manufacturers have

already solved the problem, but many have not.

The details: Section 3.3.4(b) (page 33) of the ICD-GPS-200 rev B

(30 November 1987 issue) states that the GPS Week count starts at

midnight 5-6 January 1980 UTC (Julian Date 2,444,244.500), and

that the GPS Week field is modulo 1024. This means that the week

count will roll over $1024/52 = 19.69$ years from then, or in $1980 + 19.7 = 1999$, only a few years from now. Specifically, first

rollover will occur at Julian Date $(2,444,244.5 + 7 * 1024) = 2,451,412.500$, which is midnight 21-22 August 1999 UTC.

I could find no mention of any field in any GPS message that would tell you which 1024-week cycle you were in. In the

July

1993 update of ICD-GPS-200, a note has been added (also on page

33) saying that the week number *will* roll over, and that users must account for this, but no way to accomplish this is mentioned. I take this note as further evidence that there is no way to tell, given only the signal-in-space definition as of July 1993. I have gotten some e-mail traffic indicating that, just as I had suspected, some manufacturers did realize that GPS would soon roll over, and were keeping it to themselves in the hope that the others would fall upon their swords. Not pretty.

Our supplier was dumbfounded when I raised the issue, couldn't stop thanking me for pointing it out years before rollover. They clearly feel that it could have been a life-threatening disaster for them. Every GPS-related product they had ever made would have come back for repair, under warranty, all at once. Too close for comfort. And, discovered by luck.

The firmware in all older units will have to be replaced. This would involve replacement of PROMs; some are socketed, some are soldered. New units presumably will know better than to claim dates from before they were manufactured, and/or will allow the user to directly or indirectly tell the firmware which 1024-week cycle to assume, without requiring replacement of that firmware at the second rollover, in $1980 + (2 * 1024 / 52) = 2019$ AD. Some of this equipment will still be in use then, long after the manufacturer has forgotten the product.

However, in spite of everything, not everybody will get the message, so system software will forever have to have an independent idea of what year it is, to know when to disbelieve a

receiver or receivers (they could all be wrong), and to handle

arguments between various GPS receivers (if only some are wrong).

Without a GPS Simulator, there is no way for users to test a GPS

receiver for this problem. All most users can do is to ask their

manufacturer for a solution, and also to imbue the system software with a suitable degree of skepticism about GPS receivers'

sense of time.

My intent in posting this note is to alert the entire industry to

the problem, allowing it to be solved with minimal disruption to

all. As a technical matter, the solution is quite simple. It's

the logistics that will take some years.

Joe Gwinn

Police Computer Stolen

David Kennedy <76702.3557@CompuServe.COM>

01 Jul 96 18:31:12 EDT

Courtesy of PA News via CompuServe's Executive News Service:

POLICE COMPUTER SNATCHED FROM DETECTIVE'S CAR

PA News 30 Jun 1996

Police Computer Stolen

By Tim Moynihan, PA News

>> A police computer has been stolen from a senior officer's
>>car, it was confirmed today.
>> Two youths snatched the laptop from a car being driven by
>>Detective Superintendent Brian Edwards, who investigates major
>>crimes in central London.
>> Scotland Yard declined to comment on whether there was
>>sensitive material on the computer though they stressed it was
>>"security protected".

o Taken by two youths when the car was stopped in traffic at
about
1740 hrs Thursday June 27, 1996.

o Police dismissed a report that the laptop contained
information
about two current, notorious cases, the Lawrence stabbing and
the death of
Member of Parliament Stephen Milligan, who was found naked
except for
suspenders and stockings with a plastic bag over his head and a
noose of
electrical cord around his---neck.

>> Police advice to the public is not to put valuable items on
>>the back seat, but to keep them in the boot.

[DMK: Article makes no mention to the state of consciousness of
the driver
of a police car stopped in traffic. TBFTGOGGI (there but
for....)]

Dave Kennedy [CISSP] InfoSec Recon Team Chief, National Computer
Security Assoc.

⚡ Automatically generated typos in online Sydney Morning Herald

Tom McDermott <spon@mpce.mq.edu.au>
Thu, 27 Jun 1996 19:26:06 +0200

The online Sydney Morning Herald (*) of June 28, 1996 contains the following phrases:
"arjpgicial turf" and
"The stereotypes Glover idenjjpgied go like this"

Someone has obviously done a search-and-replace to convert "tif" to "jpg" on the HTML source with the rather cryptic results above; I suspect the culprit is a single missing backslash - they've searched for '.tif' not '\\.tif'

The risk? Looking foolish by publishing nonsense.

(*) To be found at <http://www.smh.com.au/>

Tom McDermott : spon@mpce.mq.edu.au

Grammar checkers

<colville@socs.uts.edu.au>

Tue, 2 Jul 1996 08:41:11 +1000

I still treasure the following response by MS Word's grammar checker.

When it came to the following fragment:

The School reviews applications by students . . .

The checker highlighted *School reviews*, and asked:

Is this a misspelling? Is it the expression *Rigor mortis*?

[It may know better than us how effective the reviews were]

John Colville, School of Computing Sciences, University of Technology,

Sydney P O Box 123 Broadway, NSW, Australia, 2007 +61 2 514
1854

⚡ The computer is always right - again

Hugh J.E. Davies <hdavies@kzin.mon.rnb.com>

Mon, 1 Jul 96 15:07:46 BST

In [RISKS-18.20](#), "Richard S. MacDonald" <dickmac@ix.netcom.com> describes how he had trouble buying some ZIP disks because "the computer is always right", even though it was wrong.

In the UK, we have a sales tax called VAT, which is levied on most things at 17.5% (It's a lot more complicated than that, but that's outside the scope of this posting.) One of the things that it's not levied on are books, which are zero-rated. Recently, I went into my local Ford dealer to buy a workshop manual for my car. They wanted the price listed, plus VAT, since car parts are liable to the tax. I pointed out that the workshop manual was a book, and therefore zero rated, but they said that the computer had no provision for selling zero rated items. Presumably, this is because car dealers are unlikely to sell the most common zero rated items (food, children's clothing, er, books).

In the end, they manually calculated what the price had to be such that the price including VAT (which the computer insisted on adding) was the price excluding VAT, and they charged me that. Of course, this makes

their VAT accounts wrong, which the Customs & Excise (who administer VAT) take very seriously. Afterwards, I called the Customs & Excise to confirm my stance, and they said that it sounded like this dealer could do with an audit ...

Hugh

⚡ Metro Machiniste leaves train for coffee

Boyd Roberts <boyd@france3.fr>

Tue, 2 Jul 1996 12:42:26 +0200

Taking Metro line 6 in Paris from Etoile yesterday at around 9 am I arrived at Kleber and stood and watched while the station initiated departure signal sounded several times while the train didn't move. The train initiated departure/door-closure signal sounded as well but we still didn't move. Two other trains arrived on the parallel track and then departed, ahead of us, although we were on the 'primary' track. They had been diverted to the 'secondary'.

I some fit of desperation I looked out from the first carriage and saw the machiniste (driver/motorman) appear from this small cabin at the head of the train with a cup of coffee (I presume). He then entered his compartment and the train departed.

I can only assume that he was counting on the automatic re-routing of the subsequent trains. Or perhaps he signaled some sort of

problem,
while he made his coffee. Trains leave Etoile about every
minute or
less and then can be re-routed back to Etoile from Kleber to
alleviate
congestion on the platform.

As I got off at Passy I remembered the story, reported in
RISKS, about
the Victoria line Tube train that departed without its driver.
If only
I'd been so lucky.

✶ Blackmailing financial institutes - a real life story

Frank Rieger <frank@artcom.de>
Wed, 26 Jun 1996 13:35:25 +0100

The HERF-against-banks-story from the Sunday Times 3 weeks ago
was somewhat
overhyped and has a lack of facts.. I have collected some facts
on real
blackmail attempts performed in Germany on a much lower, but
maybe
comparable level.

Since February 1996 until last week a person named Markus
S=F6hnke
Ungerb=FChler was calling German banks and corporations,
claiming he was a
member of the Chaos Computer Club and has hacked the corporate
computer
system. He claimed, that he has his hands on data that proves tax
manipulations and other illegal activities of this company. He
also claimed
the hacking of several systems in main German press magazines
like stern and
Spiegel. Ungerb=FChler asked the banks and companies for paying
him some

1000 Deutschmarks for giving them the data "back". Another scheme was to ask for payment for removing allegedly planted negative-stories from the press computers. As known by now all of some dozen companies and banks paid in panic reaction for avoiding any press coverage. Only a very, very small minority of victims asked the police for help - after paying. In several cases Ungerb=FChler handed out some disks with the "data" in exchange for the money. These disks were empty.

Mr. Ungerb=FChler has escaped in February from an psychiatric hospital, where he was arrested cause of being an proven schizophrenic and blackmailer. He started his activities two days after his getaway. He based in London and operated via some Fax- and Voicemail boxes. The investigation of the case was difficult, cause none of the victims was willing to prove the identity of the blackmailer for the police etc. (Ungerb=FChler used to show money couriers from the banks his authentic passport to prove he is the right person to receive the money)

He is definitely not a member of the Chaos Computer Club and is, as far as known by now, unable to hack into computer systems. He is simply a confidence trickster.

The case shows, how fast and easy big companies pay, if they fear press coverage of real or alleged problems. They pay to everyone who believable claims to be able to perform hacking or electronic attacks.

In the light of this case, I could imagine, that around 40 banks in London

City have paid for being not attacked by HERF - without the real prove, that the blackmailers own such weapons. There is a real huge amount of irrationality in computer security issues, especially in the financial sector. It seems like no one trusts his security measures. As I have learned in this case, these security-guys are thinking all the time in a worst-case manner and if the worst case occurs they are unable to react rational. You did not need Schwartau-style doomsday-weapons for getting lots of money - ou only have to be eloquent and know the right buzzwords. Finally the Ungerb=FChler-case was mainly fixed cause of massive activities of an well-known international security company paid by one of the victims, not cause of so good cooperation between police and the victims.

Frank

(source: partly from Der Spiegel 24.6.1996,
<http://eunet.bda.de/bda/int/spon/magazin/gesel02.html>)

✶ Re: DoD and IRS tax systems (Wexelblat, [RISKS-18.23](#))

"Dennis G. Rears" <drears@Pica.Army.Mil>
Tue, 25 Jun 96 9:37:56 EDT

Richard L. Wexelblat writes:

>Special note: I work for the IRS and have a work-related
vested interest
>===== in not having the Department of Defense
involved in
> contracting for IRS software and systems.
Therefore,

> despite any claims of non-bias below, I am clearly
> "interested" in the classical sense of the word.

My special note: I work for the Army as a civilian.

>That part out of the way, I'd like to say (as a private
citizen, a
>tax-and-spend liberal, and an almost-always defender of free
speech and the
>right of the citizen to privacy) that the present initiative by
Congress to
>have DoD become the contracting agent for IRS system and
software
>development is a clear and present danger to privacy in the
Republic in
>which we stand.

I think it is funny that somebody from the IRS has the GALL to
write
about privacy worries about the DoD. This from a representative
from an
agency that wants access to all financial data from all its
citizens.
They want to know under criminal penalty about accounts outside
the US
borders. I don't even have to talk about the Social Security
Number.

>The initiative referred to above is in the "Subcommittee Mark"
of the
>proposed next year's budget. It's just a House Subcommittee so
it's not
>law, but it's a bad idea in my mind, even to consider it
seriously. Is the
>Department of Star Wars and the \$700 toilet seat really so
excellent a
>contracting agency that they are the clear choice to handle IRS
business?

Typical attack based upon ignorance. First it is the
Department of
Defense. Second, he mentions the \$700 toilet seat when in fact
it was in

the \$600 range. For those who know about the \$600 toilet seat, the cost is defensible. It was fabricated by an aircraft company at the request of the Air Force (not DoD). It was not mass produced and was made to AF specs.

The company did not even want to make it. They produced it at cost. When a company produces a small amount of items they are expensive.

I don't know the full details of the proposal. Is it the DoD, AF, or what agency that will procure the system? They do have separate procurement departments. They all operate under the FAR and DoD regulations but the AF and Army also have additional procurement regulations.

>Well, that's my biased opinion, and I'd like very much to hear from
>others who may have a more valid claim to disinterest!

Well essentially there are no facts in this post. The IRS has already shown their incompetence in procuring ADP systems. If it is not the DoD, it might go to NASA or some other agency.

Dennis

✶ Re: DOD and IRS tax systems (Wexelblat, [RISKS-18.23](#))

"Scott A. Renner" <sar@langley.mitre.org>

Tue, 25 Jun 1996 10:46:19 -0400

Where is the RISK? The term "Department of Star Wars" shows a political objection, not a technical one. The "\$700 toilet seat" outrages usually

turn out to be

(a) priced the same as comparable civilian items; eg.
aircraft coffee
makers, emergency flashlights, or

(b) priced according to procurement regulations imposed by
Congress;
\$15 for the toilet seat, \$685 for overhead

and in any case do not tell us much about software development.
True,
the history of software development in the DOD is not a happy
one, but
then the IRS hasn't done very well in the past, either. In
terms of
privacy concerns, the IRS is **much** more threatening than the
DOD. That
threat is not changed if DOD contractors start writing IRS
software.

Having DOD develop software for the IRS does not especially
strike me as
one of the best ideas of the 1990s -- but where's the RISK?

Dr. Scott A. Renner The MITRE Corporation P.O. Box 716
Langley AFB, VA 23665 USA +1 804 766-4592 sar@mitre.org

✶ Re: DoD and IRS tax systems (Wexelblat, [RISKS-18.23](#))

Carl Minie <CarlM@qsc1po.qstr.com>
Thu, 27 Jun 1996 14:12:51 -0400

As an ex-liberal and small-l libertarian, I submit that the true
danger to
privacy in the Republic is the practice of gathering detailed
financial
information from all (law-abiding) Americans under threat of
asset

confiscation and jail terms, and then giving tens of thousands of government employees access to this information in the course of their employment. I further submit that passing a few wimpy privacy laws and expecting them to prevent this information from being used for personal and political purposes is magical thinking. It doesn't take a genius to surmise that IRS data is used regularly for illegal purposes by everyone from the sitting President (of either party) down to grudge-bearing neighbors and ex-spouses. I believe the IRS attempted to assess the depth of the problem in their Southeastern Region (where my mother worked) at one time, and stopped at well over 300 violations. You or I would have ended up at Leavenworth, but all but a few of the most egregious violators were simply warned not to do it again.

You can take voluntary action to keep yourself out of the TRW/Equifax/TransUnion food chain and off junk mail lists...but Federal law requires you to remain in the IRS's gunsights for your entire productive lifespan. Neither party supports privacy when it means privacy from the government; it is a Democratic president who is enthusiastically supporting the FBI and NSA in their efforts to prevent American citizens from using encryption that they can't break, and to require that every phone, fax, and modem in the United States contain a chip that would allow government agencies to tap in at will. Do I need to add here that the very concept of economic privacy is anathema to those who believe that a portion of

everything you earn, keep, spend, or invest belongs to them, and that not handing over the fraction they demand is stealing from them?

> Is the Department of Star Wars and the \$700 toilet seat really so excellent a contracting agency that they are the clear choice to handle IRS business?

I don't expect the IRS to be abolished anytime soon...but letting the DoD design its computer systems would be an acceptable second choice. The DoD may be expensive, but they're not very good. My fondest hope is that with a spanking new Government Issue computer system, the IRS that the GSA says can't figure out where 60% of its own budget goes won't be able to find 60% of mine. I don't like paying for \$700 toilet seats (or \$320,000 spotted owls) any more than you do.

The solution which provides the smallest RISK to privacy is not to gather the data in the first place. If tax compliance is truly voluntary, then the IRS should trust that we are reading 21,000 pages of IRS rules and case law and sending in the correct amount.

Long Pig

⚡ Digital Precipice: What the computer trade hides from their customers

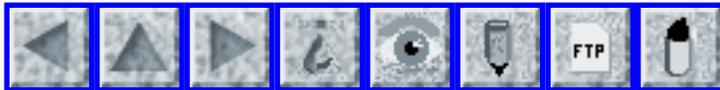
<KRach@aol.com>

Sun, 30 Jun 1996 05:48:07 -0400

In Germany a new book has been published by Markus Gaulke that

describes and illustrates (by citing hundreds of precise and real computer mishaps) the risks and dangers connected to the increasing use of information technology in all parts of human life. The book is very interesting reading, easy to understand and gives valuable insights. Unfortunately the book (344 pages) is published only in German so far (original titel: "Digitale Abgruende - Was die Computerbranche ihren Kunden verschweigt"; verlag moderne industrie, ISBN: 3-478-91510-4), but the author offers a Web Page in English about the contents of his book (<http://members.aol.com/Secuinfo/welcome.html>).

Kirsten Raach, computer consultant



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 18: Issue 25

Friday 12 July 1996

Contents

- [Western U.S. power blackout](#)
[PGN](#)
- [Recent west-coast power outage and thoughts on the power grid](#)
[Nicholas C. Weaver](#)
- [Massive cell-phone identifier interception](#)
[PGN](#)
- [56-Bit Encryption Is Vulnerable, Says Zimmermann](#)
[Edupage](#)
- [John Munden is acquitted at last!](#)
[Ross Anderson](#)
- [Risks of Computers In Automobiles](#)
[George Beuselinck](#)
- [Re: DoD and IRS tax systems](#)
[Todd B SanMillan](#)
- ["Microsoft apologizes for *offensive* thesaurus errors"](#)
[PGN](#)
- [Microsoft mail, bane of mailing list software](#)
[Joe A. Dellinger](#)
- [Re: More AOL censorship](#)
[MarkAYoung](#)

● [Info on RISKS \(comp.risks\)](#)

⚡ Western U.S. power blackout

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

Thu, 4 Jul 96 6:13:41 PDT

More than a dozen states including California, Oregon, Washington, Utah, Nevada, Wyoming, Arizona, reported power outages on 2 July 1996. At least 11 separate power plants "inexplicably were knocked off line". The problem appears to have originated at a 1500-megawatt intertie at the California-Oregon border. Later in the day, plants in Rock Springs, Wyoming, and along the Colorado river also went off line. [Source: Reuters item, *The Boston Globe*, 3 July 1996, p.3]

On the following day, parts of Idaho were again blacked out. Perry Gruber, spokesman for the Bonneville Power Administration in Portland, Oregon, said, "We can rule out sabotage. We can rule out UFOs. I think we can rule out computer hackers." Utility officials said it may take as long as a week to find the cause(s). [Source: Associated Press item, *The Boston Globe*, 4 July 1996., p.4]

[Jerry Saltzer, who was in Idaho, remarked to me that what was most striking was the sheer confusion in reports of what might have been the cause. "AP reported without comment that eleven generating plants shut down simultaneously, with the apparent implication that some kind of widespread

conspiracy was involved. Idaho Power said the problem originated in

California, but its system autoshut down completely and had to go through a

"Black Start". Oregon's main power company said it was a problem on the

Pacific Northwest Intertie. Colorado's power company said the problem

originated in their system but they didn't understand what it was. Idaho

Power said it had nothing to do with the hot weather and unusual load from

air conditioning. Oregon said it was caused by the hot weather and unusual

load from air conditioning. Three days later they still didn't have any

consensus on what had happened. Impressive disarray--one has the feeling

that they don't talk to one another. With this much lack of communication,

I'm not sure they should be allowed to interconnect, either."
JHS]

⚡ Recent west-coast power outage and thoughts on the power grid

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

Wed, 3 Jul 1996 12:56:00 -0700

[...] At least 1.5 million customers were affected by sporadic outages.

Apparently an instability in the power grid caused these problems. (It is

interesting how sporadic these outages were. In Berkeley, our power wasn't

interrupted, yet portions of the Bay Area subway system (BART) were without

power).

Other contributors can no doubt explain better than I can how such instabilities occur, but I would rather address a more frightening thought: Can such instabilities be deliberately introduced? Could someone actively sabotage the power-grid in this way?

This outage didn't cause much damage. After all, it was during the day and hot and miserable, so a few million people were simply made uncomfortable. But what would happen to LA if a California wide blackout occurred at say, 11pm on Dec. 31st?

One might also wonder if other portions of our energy infrastructure are similarly vulnerable to attack?

nweaver@cs.berkeley.edu <http://www.cs.berkeley.edu/~nweaver>

[The answer to your first and third questions is unfortunately YES, and transcend the energy infrastructure. The Senate Governmental Affairs Committee Permanent Subcommittee on Investigations, chaired by Senator Nunn, has been holding hearings that include this very topic. My testimony from 25 June is available for FTP (in PostScript form only at the moment) from ftp.csl.sri.com in the file pub/neumannSenate.PS . PGN]

⚡ Massive cell-phone identifier interception

"Peter G. Neumann" <neumann@csl.sri.com>
Thu, 4 Jul 96 8:13:41 PDT

Two people in Brooklyn NY (Abraham Romy and Irina Bashkavich) were charged with stealing over 80,000 cellular phone numbers, along with corresponding identifying serial numbers and personal identification numbers, using a scanner (digital data interceptor) from their 14th-floor windowsill above the Belt Parkway in Brooklyn. Police seized two handguns, six computers, 43 cellular phones, and the scanner. Cellular-phone fraud reportedly amounts to losses of \$1.5 million per day. [Source: An Associated Press item in **The New York Times**, 3 July 1996, p. B4]

✶ 56-Bit Encryption Is Vulnerable, Says Zimmermann (Edupage)

Edupage Editors <educom@elanor.oit.unc.edu>
Sun, 30 Jun 1996 18:01:43 -0400 (EDT)

Philip Zimmermann, creator of Pretty Good Privacy encryption software, testified before a Senate subcommittee that, based on a 1993 presentation by Michael Wiener of Northern Telecom, it would be possible to build a machine for \$1 million that could crack a message encrypted with the Data Encryption Standard and a 56-bit key in an average of 3.5 hours. A more powerful machine, costing about \$10 million, could do it in 21 minutes, and a \$100 million machine could bring the time down to two minutes. Zimmermann's testimony contradicted a recent statement by U.S. Attorney General Janet Reno that even with a "top of the line supercomputer, decoding a 56-bit key

would take over a year and the evidence would be long gone." At issue is whether the U.S. should permit the general-license export of 56-bit encryption products. (BNA Daily Report for Executives 27 Jun 1996, A5, in Edupage, 30 June 1996)

✶ John Munden is acquitted at last!

Ross Anderson <Ross.Anderson@cl.cam.ac.uk>

Mon, 08 Jul 1996 18:26:10 +0100

At twenty past two today, John Munden walked free from Bury Crown Court. This resolved a serious miscarriage of justice, and ended an ordeal for John and his family that has lasted almost four years.

In a judgment loaded with significance for the evidential value of cryptography and secure systems generally, His Honour Justice John Turner, sitting with two assessors, said that 'when a case turns on computers or similar equipment then, as a matter of common justice, the defence must have access to test and see whether there is anything making the computers fallible'. In the absence of such access, the court would not allow any evidence emanating from computers.

As a result of this ruling, the prosecution was not in a position to proceed, and John Munden was acquitted.

John was one of our local policemen, stationed at Bottisham in the Cambridge fenland, with nineteen years' service and a number of commendations. His ordeal started in September 1992 when he

returned
from holiday in Greece and found his account at the Halifax
empty. He
complained and was told that since the Halifax had confidence in
the
security of its computer system, he must be mistaken or lying.
When
he persisted, the Halifax reported him to the police complaints
authority for attempted fraud; and in a trial whose verdict
caused
great surprise, he was convicted at Mildenhall Magistrates'
Court on
the 12th February 1994.

I told the story of this trial in a post to comp.risks (see
number
15.54 or get ftp.cl.cam.ac.uk/users/rja14/post.munden1). It
turned out
that almost none of the Halifax's 'unresolved' transactions were
investigated; they had no security manager or formal quality
assurance
programme; they had never heard of ITSEC; PIN encryption was
done in
software on their mainframe rather than using the industry-
standard
encryption hardware, and their technical manager persisted in
claiming
(despite being challenged) that their system programmers were
unable
to get at the keys. Having heard all this, I closed my own
account at
the Halifax forthwith and moved my money somewhere I hope is
safer.

But their worships saw fit to convict John of attempted fraud -
which
made the national papers.

An appeal was lodged, but just before it was due to be heard - in
December 1994 - the prosecution handed us a lengthy 'expert'
report by
the Halifax's accountants claiming that their systems were
secure.

This was confused, even over basic cryptology, but it was a fat and glossy book written by a 'big six' firm with complete access to the Halifax's systems - so it might have made an impression on the court. We therefore applied for, and got, an adjournment and an order giving me - as the defence expert witness - 'access to the Halifax Building Society's computer systems, records and operational procedures'.

We tried for nine months to enforce this but got nowhere. We complained, and an order was made by the judge that all prosecution computer evidence be barred from the appeal. The Crown Prosecution Service nonetheless refused to throw in the towel, and they tried to present output such as bank statements when the appeal was finally heard today.

However, the judge would have none of it.

Many thanks to all those who helped, and especially to guys like Brian Randell, Chuck Pfleeger and John Bull who wrote in to the Chief Constable and pointed out that the original judgment was patently absurd. It was largely due to their letters that John was suspended from the force rather than sacked.

For the computer security community, the moral is obvious: if you are designing a system whose functions include providing evidence, it had better be able to withstand hostile review. This is understood by designers of forensic systems, and the value of hostile review is also well known to the military and the utilities. But with one or two exceptions -

such as SET -
the banks are just not on the same planet, and the risk to them
should be
clear!

Ross

✦ Risks of Computers In Automobiles

George Beuselinck <georgeb@mhv.net>

Thu, 11 Jul 1996 19:43:01 -0400

Just got this in from a friend at Microsoft:

DETROIT - General Motors Corp. said Tuesday it is recalling
about 292,860
Pontiacs, Oldsmobiles and Buicks from the 1996 and 1997 model
years
because of an engine software problem that could result in a
fire.

The cars are the 1996 Pontiac Bonneville, Oldsmobile Ninety
Eight and
Eighty Eight, Buick Park Avenue, LeSabre, Riviera and Regal, and
some
1997 Buick Le Sabres.

GM said a faulty engine system sequence can cause a backfire
during
start-up. That can result in a cracked intake manifold, which in
some
instances could erupt in a fire.

With the proliferation of computer technology into
automobiles, it had
to happen sooner or later...

George Beuselinck georgeb@mhv.net

✈ Re: DoD and IRS tax systems (Wexelblat, [RISKS-18.23](#))

Todd B SanMillan <bain@crl.com>

2 Jul 1996 15:03:43 -0700

My special note: I am also a tax-and-spend liberal, and in addition I have a background in the rules of logic and am a native speaker of English.

>>The initiative referred to above is in the "Subcommittee Mark" of the
>>proposed next year's budget. It's just a House Subcommittee so it's not
>>law, but it's a bad idea in my mind, even to consider it seriously. Is the
>>Department of Star Wars and the \$700 toilet seat really so excellent a
>>contracting agency that they are the clear choice to handle IRS business?

> Typical attack based upon ignorance. First it is the Department of
>Defense.

Are we really supposed to believe that the original poster was "ignorant" of this point? To me, the original poster was obviously employing "rhetoric", a common argumentative technique that adds nothing to the logical argument, merely makes a more forceful emotional appeal. It appears to have worked in this case.

> I don't know the full details of the proposal.

It is also a weak argument to accuse the poster of ignorance, then admit your own ignorance.

Next we get 2 (somewhat conflicting) explanations of "the \$700 toilet seat", from 2 different posters, one of which explains that "in fact it was in the \$600 range." I'm sorry, but this makes little difference to the weight of the argument. At \$600 a seat, it still needs explaining, a point that the poster recognizes by offering an explanation.

The RISKS? Employing emotional, rhetorical arguments while condemning them in the other side of the argument does little to help your side and keeps the noise level high.

✶ "Microsoft apologizes for *offensive* thesaurus errors"

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

Mon, 8 Jul 96 7:32:44 PDT

Microsoft Mexico has an on-line Spanish-language thesaurus that has caused quite a stir. For example, the word "Indian" was equated with "man-eater" and "savage"; "Western" with "Aryan", "white", and "civilized"; "lesbian" with "pervert" and "depraved person". Microsoft Mexico has apologized, and is rushing in a language expert from their software development center in Ireland. [Source: *The Boston Globe*, 6 July 1996, p.58.]

✶ Microsoft mail, bane of mailing list software

Joe A. Dellinger <jdellinger@amoco.com>

Sat, 6 Jul 1996 16:18:56 -0500

I maintain a mailing list using the old "listproc" package. Unfortunately, Microsoft Mail users cannot subscribe, unsubscribe, etc, except by manually sending e-mail to me. Microsoft mail (at least the way they are using it) inserts a blank line at the front of the message, then some special microsoft mail headers, and only THEN includes the text being mailed. The trouble is the list processor sees the Microsoft mail fields as the start of the message and aborts (since those aren't legal listproc commands) without reading further.

Another mailing list I subscribe to has been repeatedly "mail bombed" by microsoft mail. If a "microsoft mail server" in the path to a recipient goes down, the list address gets bombarded with error messages. The error messages then get echoed back out to the entire list and create additional error messages. The problem appears to be that "Microsoft mail" error messages don't conform to the mail protocols the list processor expects to see flagging error messages, and so are not rejected by the mailing list software.

One other annoying incident occurred on the mailing list I maintain (unrelated to microsoft mail this time!). Someone on the list decided to edit their "name" to be extremely long, like so: From: canadian_fellow@canadian_university.ca (His name followed by a very long diatribe against French nuclear testing in the Pacific here, all

on one
line!) The list processor software overflowed the field and
truncated his
diatribe. Most of the sites receiving the broadcast then barfed
with
various nasty error messages because of the mismatched
parenthesis, causing
a flood of error messages to come back to me as the list
maintainer.

⚡ Re: More AOL censorship (Reid, [RISKS-18.23](#))

MarkAYoung <markayoung@aol.com>

7 Jul 1996 23:56:32 -0400

>This clinches it. AOL customers do not pay to receive e-mail
and never have

AOL customers have a monthly allotment of time in many areas,
including MAIL
and newsgroups, and have to pay for connect time beyond their
allotment. The
standard plan has a 5-hour monthly allotment with \$2.95/hr
beyond that.

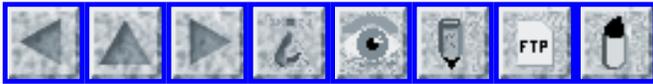
The same is currently true for CompuServe, too.

Therefore lots of spamming will cost AOL customers money if
they reach
their 5-hour montly allotment.

--Mark A. Young, MarkAYoung@aol.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 18: Issue 26

Friday 19 July 1996

Contents

- ["Primary Colors" and computer evidence](#)
[Peter G. Neumann](#)
- [The increasing complexity of everyday life](#)
[Don Norman](#)
[PGN](#)
- ["Computer Buff Raids Marks & Spencer Security Secrets"](#)
[David Kennedy](#)
- [ICEE voice-mail breakin](#)
[Thomas Insel](#)
- [NSA response to key-length report](#)
[Matt Blaze and Whit Diffie](#)
- [Re: 56-Bit Encryption Is Vulnerable, Says Zimmermann](#)
[Dave Tweten](#)
[A. Padgett Peterson](#)
- [New ATMs considered harmful](#)
[Carl Resnikoff](#)
- [Safety-Critical Computer Systems, by Neil Storey](#)
- [Info on RISKS \(comp.risks\)](#)

⚡ "Primary Colors" and computer evidence

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

Wed, 17 Jul 96 18:32:47 PDT

In [RISKS-17.75](#), Peter Wayner noted the computer study done by Professor Donald Foster at Vassar College that attributed the writing style of the anonymously authored novel ``Primary Colors'' to Joe Klein, a Newsweek columnist and CBS commentator. Recently, Maureen Casey Owens, past president of the American Academy of Forensic Sciences, studied the handwritten notes on the amended typescript pages for the novel and concluded that the handwriting was most certainly that of Joe Klein. [Source: an article by David Streitfeld in *The Washington Post*, 17 July 1996] (An NPR program I heard at lunchtime on 17 Jul noted that other investigators had turned up the fact that Klein had recently paid cash for half of the price of his new house, seemingly having struck it rich in a short period of time.) On the same day, Random House finally admitted that Klein was indeed the author.

Peter Wayner earlier had suggested in [RISKS-17.75](#) that if Joe Klein were really trying to hide his identity, he would have disguised his writing style more assiduously. But we might suspect that Joe did not want to hide his identity completely, because the suspense has undoubtedly increased sales and paid for his house, and the having been identified will now dramatically increase his name-recognition index. On the other hand, Klein is now taking a lot of flak relating to his integrity as a journalist, because until now he has lied in denying authorship. Is it really true that all publicity is good publicity, even if it is bad publicity?

So, you may ask, where is the RISKS relevance in this case?

* RISKS readers are by now accustomed to being suspicious of purported computer evidence. Here, the winnowing out of Joe Klein's identity by Professor Foster is in retrospect very impressive. A case in which such evidence turns out to be actually correct is certainly worth mentioning, particularly because RISKS is sometimes criticized for including so many negative computer-related cases (a situation that occurs largely because we so seldom see real successes). Thus, there can be risks in *doubting* that digital evidence is truthful. But, above all, there are always risks in *believing* that digital evidence is truthful.

* There is the risk of believing that you can reliably hide your identity, even in the presence of altered writing styles, veiled attacks on oneself (the novel contains ``an unflattering portrait of a reporter who

resembles

Klein, according to Streitfeld), various forms of steganography, spoofed e-mail, and a trustworthy senior editor. You must also beware of telephone records, credit-card records, airplane reservation databases, library records, nosy realtors, snoop neighbors, coincidental encounters, etc.

* The art of lying is very difficult. If you are going to attempt it, you must be prepared to be absolutely consistent forever, because otherwise inferences can be drawn that can smoke you out. However, absolute consistency is in general impossible, especially if the cover story is in any way inconsistent with perceivable reality. Cover stories with plausible deniability are best when they are also legitimate. However, with web servers and cross-linked databases, it is increasingly difficult to hide the rest of the story. Also, covert activities in the intelligence world are such that you must lie in denying the mere existence of a covert operation (which, *by definition* "does not exist"), and in the name of national security you must perjure yourself whenever you are challenged. So, beware of what can be gleaned from computer-related inferences -- especially when some of the information is perfectly above-board but perhaps not completely correct.

In this case, the Klein battle to remain anonymous may seem to have turned inside out, but the situation is now really a Klein bottle in which secrecy and full disclosure are both on the same surface and ethics have become blurred with nonethics. Stay tuned for the Klein re-bottle. I'm not taking bets.

The only consistent course is clearly to avoid putting yourself in such a position in the first place. Although that might seem to preclude April Fools' spoofs, note that in our most famous cases (for example, the Chernenko and Spafford e-mail spoofs discussed in the RISKS archives and in my RISKS book), the prankster has unabashedly 'fessed up when confronted (Piet Beertema and Chuq von Rospach, respectively), and generally received admiration for his cleverness. (The negative responses that "Chernenko" took are also worth noting.) Similarly, Robert Morris never denied his involvement in the Internet Worm experiment that went seriously awry. So, perhaps it would have been OK for Klein to publish anonymously if he had

admitted his authorship when first challenged? However, to expect that he could remain anonymous forever is totally unrealistic in our information-laden world, and that realization may color [!] future authors seeking similar subterfuges. On the other hand, to retain anonymity in order to further increase sales is either (1) morally reprehensible, or (2) just consistent with the emerging American Way -- anything is OK as long as you can get away with it, or (3) both 1 and 2.

[Peter Wayner found the following quote in Media Circus on-line, referring to Maureen Casey Owens' analysis of the Klein typescript:

Says Joshua Sostrin, "The analyst later concluded that the Declaration of Independence, as has long been suspected, was indeed penned by Bob Dole."]

🔥 The increasing complexity of everyday life

Don Norman <dnorman@apple.com>
Mon, 15 Jul 1996 10:09:42 -0800

Musings on the ever-increasing complexity of everyday life, triggered by the ever-increasing size of the "end-of-the-digest" announcement of the RISKS Digest:

I am alternately amused and terrified by the ever-increasing complexity of everyday life. Technology provides more and more functions essential to our life. More and more artifacts pervade our lives and make themselves essential to our lifestyles. Many of the new technologies involve communication networks that interconnect large numbers of systems. These lead to an increase in the complexity of societal interactions and the sheer number of contacts among people. As a result, the number of potential weak points increase, and thereby the dangers. The ever-increasing amount of interactions among people, institutions, and governments gives ever-more opportunities for disaster, and the natural tendency of governments and

institutions is to tackle each known problem by instituting rules, regulations, and laws to control the abuses. But these well-intentioned (and sometimes not so well intentioned) efforts simply proliferate to add yet more complexity to our lives.

Those in computer science know how difficult it is to disentangle the interactions of a rule-based system. What happens when the rules are those of an institution or government, designed by multiple people over decades -- centuries? We have rules that interaction unplanned ways, rules that are inconsistent. Rules that are vague and ambiguous. Rules that were relatively clear and precise in the era they were developed, but become outmoded or imprecise with the passage of time and the invention of new technologies. We all know what the result is: unstable, unpredictable systems.

Even my own home grows rapidly in complexity. 8+ remote controls to operate my home theatre/TV. An ever-increasing set of manuals for the ever-increasing number of home appliances. A dozen or so electric clocks to be reset when power fails and during the biannual summertime/regular time switch over. Items to be lubricated, adjusted, dusted, tested. batteries to be checked and replaced on a regular basis. Security precautions in the home and at work: identification badges, more secure driver's license, more secure \$100 bills, and the ever proliferation of passwords --each to be non-words, each to be changed at frequent intervals.

Even the RISKS Digest itself is not immune. Look at the end-of-the-digest announcement. Once this was a few lines, at the beginning of the digest. Then, people like me had problems with the FTP instructions, so the instructions were made more complete and precise -- but thereby longer. Then people like me kept asking for permission to reprint, so the announcement was modified to spell out the policy (which, of course, required inventing a policy). Soon, the number of items got so large that the whole thing was put at the rear of the digest, where it now takes up over a page of printed text. How long before it is two pages? How long before it rivals the size of the digest itself? [SEE NEXT ITEM. PGN]

What's the RISK? Well, as life gets more and more complex, the number of interactions increases (as N-squared? faster?). The number of unexpected interactions also increases, usually with unknown impact. We have already

seen how the interconnectedness of the phone systems and the electric utility systems means that single-point failures can sometimes bring down a large region of the country. I expect these instances to increase, both in number and in magnitude, as the number of interconnections increase.

The real question is: are there alternatives or are we doomed to ever-increasing complexity?

Don Norman. VP, Apple Research Labs dnorman@apple.com

⚡ Re: The increasing complexity of everyday life

RISKS List Owner <risiko@csl.sri.com>

Fri, 19 Jul 96 9:33:45 PDT

Don, I am really glad you raised this issue. It is worthy of considerable discussion in RISKS.

Not incidentally, a problem in the past is that RISKS gets distributed to net-lame places that cannot use the web or FTP or much else, or in some cases cannot even reply by e-mail. The full risks.info message kept growing in part to stave off all of the victims of noncompliant Internet service providers and sites without webservers. I too have been annoyed at the increasing volume of the risks info message. So, thanks to your urging, from now on new subscribers will continue to get the full info page initially when their subscription is acknowledged, and the regular end-of-issue item will be BRIEF. The full info message can be gotten by e-mail to risks-request@CSL.sri.com with the one line INFO, by ftp, and as a web page, and the brief message (see the end of this issue) states that "All contributors are assumed to have read the full info file." I hope that suffices. MANY THANKS for the prompt. PGN

⚡ "Computer Buff Raids Marks & Spencer Security Secrets"

David Kennedy <76702.3557@CompuServe.COM>

10 Jul 96 19:08:36 EDT

PA News 7/10/96 12:39 PM

>> A computer buff who downloaded the Marks & Spencer's security
>>file containing pin numbers when he visited a London store to
>>carry out maintenance, was ordered to complete 70 hours
>>community service work today.

>> Former Olivetti computer engineer Edward Yearley, 29, of
>>Vicarage Lane, Bovington, Hemel Hempstead, Herts, was convicted
>>in June of gaining unauthorised access to computer material in
>>October 12 1994, under the Computer Misuse Act 1990.

o Yearly posted the file to the "Gates of the Underworld" BBS where it
was noticed in November. Police duly executed a search warrant on his
home, seizing his PC and disks. Yearly denied belonging to the BBS, but
his
computer showed where he had uploaded the file under the pseudonym "Mr.
Ed."

>> After reading pre-sentence reports magistrate Paul Clark
>>said: "There is an element of breach of trust here. It is fair
>>to say a certain amount of knowledge and expertise is needed to
>>commit an offence such as this."

[DMK: I don't know whether to sigh or barf.]

>> He added: "I'm satisfied there was no question of personal
>>profit for you, no gain and no loss to Marks & Spencer. But
>>the scope for other people to misuse the information that was
>>downloaded is hard to judge."

o Yearley was ordered to perform 70 hours of community service and pay
UKP170 in cour costs. His computer will be returned to him.

>> "Although your own personal computer was seized and evidence
>>gathered from it, your own computer was not used for committing
>>the offence or facilitating it."

[DMK: Stealing the data in the first place and violating the Parker
principle of Possession or posting it to the BBS and violating the
principle
of Confidentiality? Maybe I'll barf after all.]

Dave Kennedy [CISSP] InfoSec Recon Team Chief, National Computer
Security Assn

⚡ ICEE voice-mail breakin

Thomas Insel <tinsel@jaka.ece.uiuc.edu>

Thu, 11 Jul 1996 02:52:24 -0500

An article in the 10 Jul 1996 **San Francisco Chronicle** (p. A13 of the East Bay edition) describes a group of high-school students who broke into a drink manufacturer's voice-mail system, erased information, changed passwords, created new accounts for their own use, and eventually crashed the system through overuse. The article reports that the company had to spend \$40,000 to bring in an outside technician and upgrade their software.

A few questions remain. Should superuser functions like the creation of new users be allowed via the phone at all? How was the infiltration so pervasive that they couldn't just shut the system down, erase bogus accounts, and change privileged passwords?

I'm reminded of a similar, more limited, incident which occurred five or six years ago when my high school set up a voice mail system to keep parents informed of their children's homework assignments. There was a system-wide password to update the information, which was changed monthly for security reasons -- in January, it was 1111, in February it was 2222, and in December it was 1212. After the system was broken into, its administrator decided against changing the password. Her reasoning: it was near the end of the month, and the password would be changed soon, anyway.

Tom Insel

⚡ NSA response to key-length report

Matt Blaze <mab@research.att.com>

Thu, 18 Jul 1996 12:08:21 -0400

18 July 1996

There is currently being circulated, to members of Congress and possibly elsewhere, a four page document entitled ``Brute-Force Cryptanalytic Attacks'' that calls into question some of the conclusions of the ``Minimum Key Lengths for Symmetric Ciphers'' white paper [1]. The document bears no author or organization attribution, but we are told that it originated from NSA.

The NSA document argues that ``physical realities'' make parallel key search much more expensive and time consuming than our white paper estimated. However, the NSA document appears to have been written from the perspective of general parallel processing or cryptanalysis rather than exhaustive key search per se. It ignores several elementary principles of parallel processing that apply specifically to exhaustive key search machines of the type that our white paper considered.

In particular, NSA argues that interconnections, heat dissipation, input/output bandwidth, and interprocessor communication make it difficult to ``scale up'' a key search machine by dividing the task among a large number of small components. While these factors do limit the scalability of more general purpose multiprocessor computers (such as those made by Cray), they do not apply at all to specialized exhaustive key search machines. The NSA argument ignores the most fundamental feature of brute-force key search: the processors performing the search have no need to communicate with other components of the system while they perform their share of the search, and therefore the system has no need for any of the global interconnections that limit scaling. Indeed, there is no reason that all the components of a parallel search machine must be located even within the same city, let alone the same computer housing. We note that one of our co-authors (Eric Thompson, of Access Data, Inc.) designs and builds medium-scale FPGA-based key search machines with exactly this loosely-coupled structure, and

regularly uses them to recover keys for clients that include the FBI.

The NSA document also calls into question our cost estimates for ASIC components, suggesting that ASIC chips of this type cost NSA approximately \$1000.00 each. However, our \$10.00 per chip estimate is based on an actual price quote from a commercial chip fabrication vendor for a moderate-size order for an exhaustive search ASIC designed in 1993 by Michael Wiener [2]. Perhaps NSA could reduce its own costs by changing vendors.

Finally, the NSA report offers estimates of the time required to perform exhaustive search using a Cray model T3D supercomputer. This is a curious choice, for as our report notes, general-purpose supercomputers of this type make poor (and uneconomical) key search engines. However, even the artificially low performance results for this machine should give little comfort to the users of 56 bit keys. According to NSA, 56 bit keys can be searched on such a machine in less than 453 days. ``Moore's law'' predicts that it will not be long before relatively inexpensive general-purpose computers offer similar computational capability.

/s/ Matt Blaze
Whitfield Diffie

References:

- [1] Blaze, M., Diffie, W., Rivest, R., Schneier, B., Shimomura, T., Thompson, E., and Wiener, M. ``Minimum Key Lengths for Symmetric Key Ciphers for Commercial Security.'' January 1996. Available from <ftp://ftp.research.att.com/dist/mab/keylength.txt>
- [2] Wiener, M. ``Exhaustive DES Key Search.'' Presented at Crypto-93, Santa Barbara, CA. August 1993.

=====
[Transcription of document circulated to various members of congress and others in June, 1996, apparently by NSA]

BRUTE-FORCE CRYPTANALYTIC ATTACKS

Two published theoretical estimates of cost versus time to perform brute-force hardware attacks on selected cryptography key lengths differ between themselves and differ significantly from what we find when we buy or build computers to carry out such attacks.

The differences lie in assumptions made in the theoretical estimates,

which are not fully spelled out by the authors, and in scaling up hypothesized small machines to ever larger ones without accounting for physical realities.

The factors not accounted for are:

- o R&D costs for the first machine, typically on the order of \$10 million.
- o As more and more chips are added to a machine, two effects occur:
 - o Interconnections increase and increase running time;
 - o Heat from the chips eventually limit [sic] the size of a machine.
- o Memory costs are not included.
- o When get [sic] to the very fast processing speed estimates, machines can become Input/Output bound; so [sic] it cannot achieve the estimated speed.
- o Assuming every algorithm can be tested in same amount of time and key length is the only difference.

Table 1 are [sic] the average time estimates made for a given cost done by Michael Wiener of Bell Northern Research in 1995. These are published in Bruce Schneier's Applied Cryptography book.

Note that these are average times, one-half of the total exhaust time.

Table 2 are [sic] the estimates for total exhaust times using Field Programmable Gate Arrays (FPGA) and Application Specific ICs (ASICs) done for the Business Software Alliance by Blaze, Diffie, Rivest, Schneier, Shimomura, Thompson, and Wiener in 1996. In addition to the above factors not accounted for they have assumed ASICs cost as low as \$10. We find ASICs more typically cost \$1000 and their capabilities can vary considerably depending upon the specific task.

Table 3 are our estimates based on our experience with a Cray T3D supercomputer with 1024 nodes. This machine costs \$30 million.

[Tables 1, 2, and 3 not transcribed here.]

🔥 Re: 56-Bit Encryption Is Vulnerable, Says Zimmermann (Edupage,

18.25)

Dave Tweten <tweten@gilmore.nas.nasa.gov>

Fri, 12 Jul 1996 13:09:53 -0700

The "Edupage Editors" make a critical mistake of logic in an item in [RISKS-18.25](#). The item reports on Philip Zimmermann's testimony before the Senate. In his testimony, Zimmermann discussed a well-known Michael Wiener paper on the feasibility of building a DES cracking machine.

The RISKS item correctly states that a \$100 million version of the machine could (according to Wiener) crack a DES key in about two minutes. Wiener's hypothetical machine is composed of a parallel array of custom designed DES cracking chips. It is by no means a general purpose computer. Still, the RISKS item says, "Zimmermann's testimony contradicted a recent statement by U.S. Attorney General Janet Reno that even with a 'top of the line supercomputer, decoding a 56-bit key would take over a year and the evidence would be long gone.'"

There is no contradiction at all. One is a "machine" that may not even qualify as a programmable computer. A "top of the line supercomputer" should not be expected to be anywhere near as effective a DES cracking engine as would be a machine such as Wiener's, built for the task out of custom chips.

🔥 Re: 56-Bit Encryption Is Vulnerable, Says Zimmermann (Edupage, 18.25)

"A. Padgett Peterson" <PADGETT@hobbes.orl.mmc.com>

Sat, 13 Jul 1996 9:54:14 -0400 (EDT)

I love how politicians can find ways to say what they want people to believe
- actually both are right. It *would* take a supercomputer a year.

However

as long time readers know neither I nor Michael have been suggesting supercomputers, instead boolean sieves (could use DSPs) made up of cascadable arrays of single bit processors were what I would use.

Similar to

parallel processors but much simpler hence faster.

The state of the art today is about 300 million keys per second for a single

sieve. Of course for a few more dollars you can set up a parallel array of

sieves, as many as you wish (initial value can be distributed and once cranking

you need not be concerned about intercommunication, a single bit would do for success).

Actually, the hard part is testing for success - of course if you have known

plaintext as most cryptographers always assume...(can think of several ways

to avoid that).

Other problem is that you also must know the exact algorithm being used - DES of course is fixed (FIPS PUB 46(A|B|C)) but a DES machine would not work

- you would need a different one - for COAST. Not difficult, just different.

Of course if you knew the target were using ENTRUST...

Now I am just an amateur cryptographer just as I have not done any serious

digital design for years, still have a pretty good idea what sub-micron lithography is capable of so know the numbers above are supportable. I do disagree with the designated heros of the MIT 7 on one point, they got the

economics wrong - while their per-wafer price is possible, the total design

would cost a bit more and there would be overhead involved (maybe governments do not worry about that but I do).

My current feeling is that 56-bit DES is OK today for a corporation so long

as every message is encrypted (including the trivial ones), each key is only

used once, and a good random key generator is used. Know that relying on high volume to raise cost-to-break vs value-of-break above buying an employee is "Security by Obscurity" but is real cost/benefit. More (64 bits)

is better and many of today's computers have granularities of 32 or 64 bits
(something I never see mentioned - design steps beyond 64 are 96 and then 128).

Padgett

P.S. I was confining my thoughts to symmetric message keys - asymmetric keys

and algorithms that may be used for key exchange are an entirely different

subject. (Have seen the two confused. Often.).

⚡ New ATMs considered harmful

Carl Resnikoff <carl@weblogic.com>

Sun, 14 Jul 1996 21:11:24 -0700

My local grocery store recently installed a kiosk with the newest generation of automatic teller machine from Wells Fargo Bank. This ATM has a high resolution color graphic display, with a touchscreen and virtual keypad for entering the PIN number.

I was standing in line about 6 feet behind the person currently using it when I noticed that each time they entered a digit on the keypad, that digit and only that digit lit up, so I could clearly make out each digit of their PIN as they pressed it, as could anybody walking by. Somehow I think this negates the value of using a PIN, when anybody within a 10 foot radius can read it without even meaning to.

Carl Resnikoff WebLogic, Inc

⚡ Safety-Critical Computer Systems, by Neil Storey

N Storey <neil@eng.warwick.ac.uk>

Mon, 15 Jul 1996 14:48:46 +0100 (BST)

Addison-Wesley, ISBN 0-201-42787-7

<http://www.eng.warwick.ac.uk/~neil/safebook.htm>

This is an introductory text covering all aspects of the development of Safety-Critical Computer Systems. It is intended for undergraduate and postgraduate students, and for engineers who use microcomputers within real-time embedded systems. It assumes no prior knowledge of safety, or of any specific computer hardware or programming language.

The book covers all phases of the life of a safety-critical system from its conception and specification, through to its certification, installation, service and decommissioning. It provides information on how to assess the safety implications of projects, and determine the measures necessary to develop systems to meet safety needs. It gives a thorough grounding in the techniques available to investigate the safety aspects of computer-based systems and the methods that may be used to enhance their dependability.

The book uses cases studies and worked examples from a wide range of industrial sectors including the nuclear, aircraft, automotive and consumer products industries. The approach taken is equally suited to engineers who consider computers from a hardware, software or systems viewpoint.



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 18: Issue 27

Tuesday 23 July 1996

Contents

- [Problems with Olympic Information System](#)
[Edupage](#)
- [Re: *Primary Colors* and Joe Klein](#)
[Joel Garreau](#)
- [Ariane 5 failure: specification and design flaws](#)
[Pat Lincoln](#)
- [Remote software changes are here](#)
[David Cassel](#)
- [*The Logic of Failure*](#), [Dietrich Doerner](#)
[PGN](#)
- [Addendum to the complexity of everyday life](#)
[Don Norman](#)
- [Re: The increasing complexity of everyday life](#)
[John Pescatore](#)
- [Re: Western power outages](#)
[PGN](#)
[Jonathan Corbet](#)
[Tracy Pettit](#)
- [Re: 56-Bit Encryption Is Vulnerable](#)
[Barton C. Massey](#)
[Steven Bellovin](#)

● [Centre for Software Reliability: Design for Protecting the User](#)

[Pete Mellor](#)

● [Info on RISKS \(comp.risks\)](#)

✶ Problems with Olympic Information System (Edupage, 23 July 1996)

Edupage Editors <educom@elanor.oit.unc.edu>

Tue, 23 Jul 1996 17:04:28 -0400 (EDT)

The "Info'96" IBM computer system designed to deliver instantaneous results of Olympic competitions to the worldwide press is working for journalists in Atlanta but not for the journalists worldwide who are supposed to be getting information from the World Press Feed. Some journalists are angrily referring to the "Info'96" system as "Info'97." An IBM spokesman said that "we expect people to judge us from our performance over the long haul of the games, instead of the first two days." Results are available quickly over the site maintained by IBM at < <http://www.atlanta.olympic.org> >. (*Atlanta Journal-Constitution*, Atlanta Games, p25) [presumably 22 July 1996]

[See also a fine article by Jerry Schwartz in *The New York Times*, 22 July 1996, C1 in the National edition. This situation was attributed to ``start-up problems.'' Jerry's article noted that ``Olympic technology officials were organizing a manual results system, part of which the ancient Greeks might have appreciated. Results are to be transmitted by facsimile

machines from outlying venues to a central office and distributed by runners.' ' The article also noted the 12-minute blackout at the Georgia Dome during Saturday night's Dream Team appearance -- blamed on a technician who pulled the wrong switch. Transportation problems are also quite severe, and cellular telephone systems were seriously overloaded at the opening ceremonies. I presume everything will be ironed out nicely just in time for the final ceremonies. PGN]

✉ Re: ***Primary Colors*** and Joe Klein (PGN, [RISKS-18.26](#))

Joel Garreau <garreau@well.com>
Sun, 21 Jul 1996 06:48:04 -0700 (PDT)

PGN makes excellent points about the difficulty of living a lie in his report on Joe Klein being unmasked as the author of "Primary Colors." But as the editor of **The Washington Post** team that had a lot of fun and a lot of pain reporting the "Primary Colors" story, allow me to cough a little dryly about the positive spin you put on the role of computers in the eventual success of our efforts.

For openers, the lesson I drew from my experience was that I would **never** trust a computer text analysis again. We ran a massive such effort independent of Professor Foster and **New York** magazine, and ours turned up results that at the time seemed fascinating, but in retrospect were

ludicrous.

Even Foster didn't trust his results enough to bet the ranch on it. As recently as the day we finally broke the story, he was saying he thought it was Klein plus somebody else, and was still berating *New York* magazine for editing into his copy the flat statement that Klein was the author. Said flat statement was inserted by an editor with no special computer experience. Klein, however, first achieved note as a political columnist for the very same *New York* magazine. I suspect, therefore, that human intuition if not specific knowledge had more to do with that piece than the computer did.

We at *The Post* *did* get a frightening amount of financial information on Klein and his wife by computer, including the cost of his house, the amount of his mortgage, his address, his previous address, everything there is to know about his cars, and so forth. And we did it in a startlingly short period of time. It's amazing what you can do when you have a person's social security number and date of birth, and equally sobering how easy it is to get that information. Only our sense of journalistic propriety prevented us from pursuing and using further information that was readily available. But again, the information so gathered ended up being largely tangential to the final report.

I find it marvelous that what finally broke the case was good old-fashioned, if imaginative, gumshoe reporting. David Streitfeld, a Washington Post

reporter with eclectic literary interests, receives all sorts of snail-mail catalogues from tiny second-hand bookstores. He saw offered for sale a copy of the manuscript...and the rest you can read in your newspapers. The handwriting analyst was an expert human. No computers were significantly involved.

Also, the reason Klein is in hot water today is that back when the *New York* article ran, we had our junk-yard dog, my boss, David Von Drehle, put him up against the wall by reminding him that credibility is the only asset a journalist has. Von Drehle than asked him to swear on his journalistic credibility that he was not the author of "Primary Colors." That's when he most memorably lied, as Klein himself acknowledged at his press conference.

In short, we put an extraordinary amount of computer effort into this story, including a passworded spreadsheet to keep track of all our reporting. But the cyberheroics ended up at best a sideshow if not a distraction, at least in our experience.

It finally was cracked and developed by old-fashioned means.

Joel Garreau

[And in subsequent elections, Joe may now be saddled with Primary Collars.

Somehow, I am reminded of a quote from the cast party after the final episode of an early TV serial, Peyton Place, in which one of the actors who had been on the show longest was asked,

``To what do you owe your success in acting?''

The answer was this:

``Honesty. Once you've learned how to fake that, you've got it made.''

PGN]

✶ Ariane 5 failure: specification and design flaws ([RISKS-18.24](#))

Pat Lincoln <lincoln@csl.sri.com>

Tue, 23 Jul 1996 10:55:22 -0700 (PDT)

A recent press release contained a good quote about the cause of Ariane 5

failure. The key 2 sentences were these:

> The failure of Ariane 501 was caused by the complete loss of
> guidance
> and attitude information 37 seconds after start of the main
> engine
> ignition sequence (30 seconds after lift-off). This loss of
> information was due to specification and design errors in the
> software
> of the inertial reference system.

The full text is at

<http://www.esrin.esa.it/htdocs/tidc/Press/Press96/press33.html>

✶ Remote software changes are here

David Cassel <destiny@wco.com>

Fri, 19 Jul 1996 20:46:29 -0700

Tonight when I logged onto AOL, I was told something like "New

Features!

America Online is being updated." They then downloaded a software change.

What's disturbing is they didn't give a chance to opt out of the upgrade

first. (The disclaimer wasn't readable. All but a corner of the text block

was hidden behind the "Welcome" screen as the bar indicating "download in

progress" snaked its way to 100%...at which time the disclaimer vanished.)

***The Logic of Failure*, Dietrich Doerner**

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

Fri, 19 Jul 96 14:41:37 PDT

Dietrich Doerner

The Logic of Failure:

Why things go wrong and what we can do to make them right
Metropolitan Books (Henry Holt), New York, 1996

[Auf deutsch war es vorher: Dietrich D\{"o}rner,
Die Logik des Misslingens, Rowohlt, 1989.]

This is a book that appeals to me very much because of its system-oriented

viewpoints. ``Faced with problems that exceed our grasp, we pile small

error upon small error to arrive at spectacularly wrong conclusions. We too

often ignore the big picture and seek refuge in what we know how to do --

fiddling while Rome burns.' ' The problems under consideration are largely

not computer problems, but the lessons are all generally relevant to RISKS

readers.

Of some importance here is the logic of analysis, which in this case includes some creative simulation studies of very diverse failures -- among which are some that are familiar to RISKS readers. The results are quite far reaching. The book provides a very interesting quasimathematical approach. The author is a distinguished German researcher, professor of psychology at the University of Bamberg, and winner of the Leibniz prize.

✶ Addendum to the complexity of everyday life ([RISKS-18.26](#))

Don Norman <dnorman@apple.com>

Sun, 21 Jul 1996 11:14:25 -0700

As an addendum to my original posting, I'd like to recommend an excellent, just published book, that describes many aspects of the ever-increasing complexity of everyday life:

Tenner, E. (1996). Why things bite back: Technology and the revenge of unintended consequences. New York: Alfred Knopf (www.randomhouse.com/).

The main emphasis is on the unintended side effects of human introduction of items alien to the culture or environment -- this includes new technologies, but also natural things such as the eucalyptus tree imported into Southern California) or the kudzu, introduced into the southeast United States. Or the computer, supposedly an enhancement of productivity, but instead a time sink. Or ...

Table of contents:

1. Ever since Frankenstein
2. Medicine: Conquest of the catastrophic
3. Medicine: Revenge of the chronic
4. Environmental disasters: Natural and Human-made
5. Promoting Pests
6. Acclimatizing pests: Animal
7. Acclimatizing pests: Vegetable
8. The computerized office: The revenge of the body
9. The computerized office: Productivity puzzles
10. Sport: The risks of intensification
11. Sport: The paradoxes of improvement
12. Another look back, and a look ahead.

Donald A. Norman, VP Apple Research, Apple Computer, Inc MS 301-4D, 1 Infinite Loop, Cupertino, CA 95014 +1 408 862-5515 <http://www.atg.apple.com/Norman/>

✶ Re: The Increasing Complexity of life

John Pescatore <johnp@tis.com>

Tue, 23 Jul 1996 08:46:27 -0400

I think increasingly complexity is an inevitable result of our nature as tool builders and users. Most animals (non-domesticated type) have very non-complex lives: find food, eat, find food, eat, sleep, procreate - kinda like folks who retire to swinging retirement communities in Florida.

As humans developed tools, they found all kinds of things to do with the tools: cook food, build shelter, develop polyester to construct leisure suits to support the pursuit of procreation, etc. We could have

simply used
the tools to increase sleep time, much the way computers were to
increase
our leisure time, but our nature seems always to lead to the
building of
things (or as George Carlin calls it, "stuff") which then
demands the
maintenance of things. This feeds the complexity upward spiral,
since the
old things never seem to go away and constantly interact with
the new things
in odd ways. Witness voice mail.

>From a Risks perspective, I think increased communications
paths mitigates
many risks. In my experience on the system engineering side of
software
development, most bugs occurred at interfaces, either between
systems or
subsystems, or between people or organizations. While one
approach might be
to eliminate interfaces, the end result is a lot more work
inside each
element. My life would be less complicated without a telephone,
but I would
spend a lot of time calculating what I could find out in one
phone call. I'm
not sure which scenario is more complex or more error-prone.

Putting big pipes between elements and maximizing
interconnections can
certainly lead to unpredictable results, but we can rarely
predict the
future anyway, so outside of relatively small systems
unpredictability is
not always bad. I think the United States melting pot model was
an example
of a highly interconnected system that lead to many
unpredictable results -
what war simulation would have predicted a recovery from Pearl
Harbor? I
fear that as American society swings back towards a less
interconnected set

of systems/cultures, many risks and interface errors will emerge with serious consequences. Similarly, any business that tried to reduce, rather than increase, its level of "connectiveness" would be a very risky investment.

John Pescatore, Trusted Information Systems, 3060 Washington Road
Glenwood, MD 21738 301-854-5710 johnp@tis.com 301-854-5363
(fax)

✈ Re: Western power outages ([RISKS-18.25](#))

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

Sun, 21 Jul 96 21:07:05 PDT

In [RISKS-18.25](#), I noted the Western power outages of 2-3 July 1996, and Jerry Saltzer commented on the evident confusion among the differing reports of what might have happened.

It took until 20 July 1996 -- 18 days later -- for the cause to be identified officially: an Idaho transmission line that short-circuited when electricity jumped to a tree that had grown too close. The tree, which has since been removed, caused a flashover in an area about 100 miles east of the Kinport substation in southeastern Idaho. The line carried 345 kilovolts. [Source: Associated Press item in the *San Francisco Sunday Examiner and Chronicle*, 21 July 1996, p.A-8.]

[I did not hear anyone say, ``Of course, we've fixed everything and it will never happen again.''] (But I thought I heard that in the

1960s.)]

⚡ Re: Western power outages ([RISKS-18.25](#))

Jonathan Corbet <corbet@stout.atd.ucar.edu>

Fri, 12 Jul 1996 09:02:36 -0600

Just a quick pointer: for those of you interested in how power outages like the one we experienced could happen, I highly recommend getting and reading a copy of "Brittle Power" by Amory Lovins and Hunter Lovins. I found it to be a high-quality discussion of a certain class of technology-related risks -- the failure modes of our energy distribution systems.

Jonathan Corbet, Nat'l Center for Atmospheric Research,
Atmospheric Technology

Division <http://www.atd.ucar.edu/rdp/jmc.html> corbet@stout.
atd.ucar.edu

⚡ Re: Western power outages ([RISKS-18.25](#))

tracy pettit <tnpetti@nppdnet.com>

Fri, 19 Jul 96 08:32:19 CDT

The United States has two major power grids. The Eastern and the Western, split approximately along a line passing through the Nebraska, Colorado/Wyoming border. The Western grid is complicated by the population pattern of the western U.S. The grid there tends towards a large "donut". The two grids are tied together by a few relatively small DC

ties.

This is not the paltry amounts of electricity flowing through the wires in your walls, or even down your neighborhood alleys. This is the massive amounts of POWER used by the entire sections of the U.S. each second. The physics and engineering involved covers multiple college courses.

The power flows according to the laws of physics, not according to who is selling how much to whom. For any given load level, the grid systems have many bottlenecks. Power companies go to great lengths to constantly balance generation to minimize these problems. Take a couple of lines out of the grid (an overload, or a fallen tree, a local storm, or just plain equipment failure), and if conditions are right, as the power attempts to get to the load, remaining lines become overloaded, protection systems open circuit breakers before the equipment can "burn down", which either causes outages (relieving the load), or causes more overloads as the power instantly takes other routes through the grid. As the outages mount, you have generators creating massive amounts of power with no place for it to go. The generators own protection systems knock them off line before they damage themselves and the humans around them. Enough generators trip off, and now you have load not being served, so it attempts to flow from the remaining generators, overloading more lines, etc. (And you thought all those dominoes were impressive.) This energy is flowing at a significant portion of the speed of light. These "system disturbances" can occur in seconds,

crossing the boundaries of all interconnected utilities in 2 blinks of an eye. A unit trip in one part of the grid can cause problems in another part, without affecting the intervening portion.

Now try and do a post-mortem on this. You have hundreds of pieces of electric power system equipment changing state, logged by multiple (several hundred ?) computer systems at numerous utilities all using separate clocks (you need to figure the sequence timed in fractions of a second).

Yes, utilities talk to each other, but even our computers can't talk that fast or accurately. Reliability costs money, and that has to come out of the electric rates. Nobody is willing to pay for us to have the constant, instant type of communications necessary to be able to determine the cause of a large outage such as this. It also costs money to get all this information and people from across the U.S. together to figure out what happened. Is it worth it? The initial reports are most likely each utility trying to make a determination looking at it from their end of the pipe.

Utility rates have always been partly a balance of reliability versus economics. Now throw the Federal Energy Regulatory Commission (FERC) and their brand new rules 888 and 889 into the mix. This is driven entirely by an idea to lower rates by increasing competition, with very little consideration for the cost of reliability. These rules are very lengthy and complicated, but one of the many requirements is that it

requires our Transmission System Operators and our Energy Marketers (who buy and sell bulk power, determining generation levels) to not have any contact with each other except through computer bulletin boards called Open Access Same-Time Information System (OASIS) . They cannot even see each other at the coffee machine. Any contact between these people has to be reported on the OASIS (this is not interpretation; it is in the rules). In an area that is basic to our reliability operations, we can no longer talk to ourselves, much less other utilities. Also, we have to allow anyone with power to market (who knows where they got it) equal access to our transmission systems. The transmission paths (even though you cannot herd electrons) are bought and sold via the OASIS. This is all driven by Independent Power Producers and intermediate Power Brokers with the idea that more competition will lower rates. You may have read about "open access" in the newspapers. To keep the transmission system owners from giving preference to themselves or anyone else (equated to "insider trading"), all information about our transmission system capabilities has to be posted on the OASIS, including any engineering studies used to determine those capabilities. All using ``standard'' Internet methods with Internet connections. Yes, the word *Internet* is used in the rules. These transmission paths do not go cheap. We are talking about millions of dollars of transactions a day being done over the Internet.

Volumes have been written and discussed in Internet Forums about the possible repercussions to the electric power industry. FERC is not to be swayed. They say they did it with the gas industry and the telecommunications industry. Gas can be stored and controlled with valves.

Telecommunications is point to point. Electric power is instantaneous, and "pooled" into the grids. They just don't seem to get it. In some places rates will drop. In others where they are already low, they will rise. Everywhere as utilities cut corners to "compete", reliability will go down.

It was asked if our energy infrastructure is vulnerable to attack? Anyone with a \$US buck-three-ninety-eight to buy a power brokers license and a copy of NetScape can surf the net and get access to the "OASIS" sights. With a college minor in Electrical Engineering you can deduce the major power bottlenecks in the power grids. Most of the transmission system lies in very remote or rural areas. [...]

Anybody see the 17 July 1996 issue of *USA TODAY*? Page 2 has an article talking about how the President of the U.S. is concerned about the security of the infrastructure, including the Internet and the power grids. It could get a whole lot worse.

It has been said that my view is alarmist. I've read the rules (I have to write programs to help my company conform), and I have 20 years experience with electric power companies. Please, somebody prove to me I'm wrong.

Tracy Pettit

✂ Re: 56-Bit Encryption Is Vulnerable (Peterson, [RISKS-18.26](#))

Barton C. Massey <bart@time.cirl.uoregon.edu>

19 Jul 1996 19:18:04 GMT

Several articles in [RISKS-18.26](#) discussed the conclusion of a blue-ribbon panel that DES's 56b key is vulnerable to brute-force attack. This issue is, to me, totally surreal; I am frightened by the way US policy decisions are being made.

As I understand it, the panel's motive in making the argument that DES is vulnerable to brute-force attack is **not** to encourage people to switch to better ciphers. Instead, it is to argue that DES should be exportable, since NSA can easily and cheaply break it!

IMHO two key facts ignored by this argument are:

1) Everybody in the world already has access to DES. Exporting it will give no one any technology access they don't already have.

2) Two-key 3DES, with its near-112b effective keylength, is **way** outside any brute-force attack I have ever heard of. Anybody with unbundled DES software or with 3 pieces of DES hardware can trivially use it to do 3DES.

NSA seems to fear that bundling DES in popular American software products will encourage routine use of good cryptography both inside and

outside the
US; this makes traffic analysis much harder for them, and thus
requires them
to expend much more effort on decryption. This is a legitimate
concern, and
deserves analysis in its own right -- it's a much more a moral,
social, and
political question than a technical one.

To phrase the debate in terms of details of the cost of
specialized
brute-force DES attack hardware is, in my opinion, absurd. As
near as I can
tell, because of facts 1 and 2 above, such hardware is
irrelevant to the
real argument, whether it costs \$100M or \$1.00.

Bart Massey bart@cirl.uoregon.edu

✉ Re: 56-Bit Encryption Is Vulnerable (Peterson, [RISKS-18.26](#))

Steven Bellovin <smb@research.att.com>

Sat, 20 Jul 1996 04:06:31 -0400

Padgett Peterson wrote:

Actually, the hard part is testing for success - of course
if
you have known plaintext as most cryptographers always
assume...(can think of several ways to avoid that).

It's pretty trivial, in fact; one can do probable plaintext
attacks. David
Wagner and I wrote a paper a couple of years ago on a
programmable plaintext
recognizer, designed to fit onboard a Wiener chip machine
(<ftp://ftp.research.att.com/dist/smb/recog.ps>). All it demands
as input is
statistical samples from the same distribution -- it worked just

fine on
both English text and executable files.

I also have a new paper -- not yet quite available, but it will be in <ftp://ftp.research.att.com/dist/smb/probtxt.ps> in a week or two, I think -- presenting an analysis of the probable plaintext available to the attackers of the IPSEC protocols. Even in a single packet, plenty of information is available, it turns out; if the attacker can use traffic analysis to identify two packets from the stream and has a suitable cracking chip (say, two Wiener engines on a single chip, with their plaintext outputs fed to the comparator under a programmed mask), the problem is trivial.

Centre for Software Reliability: Design for Protecting the User

Pete Mellor <pm@csr.city.ac.uk>
Tue, 23 Jul 96 11:18:43 BST

CSR, Centre for Software Reliability
THIRTEENTH ANNUAL WORKSHOP
DESIGN FOR PROTECTING THE USER
The Grand Hotel, Burgenstock, Switzerland
11th-13th September, 1996.

This is a brief summary of the programme. The complete version, including full registration details and electronic booking form, is available on the WWW at URL:-

<http://www.csr.ncl.ac.uk/clubs/burgenstock.html>

CSR home pages can be found at <http://www.csr.city.ac.uk:8080/>

and <http://www.csr.ncl.ac.uk/>

Who should attend?

The workshop will deal with a number of topics that are regularly aired on the RISKS forum, and should be of great interest to all readers of, and contributors to, RISKS.

It is intended for researchers, requirements owners and system designers who are concerned with issues of protecting people from the consequences of faulty and unsuitable computer and information systems.

Workshop theme

In the talk about making the roads of information safe and secure, many wider social issues are ignored in the focus on technical solutions to technical problems (secure protocols, trustworthy authentication, encryption of confidential data and so on). Examples include people who have had their creditworthiness destroyed or been made bankrupt or rendered homeless by misuse or misinterpretation of data, and many computer systems cannot adapt to human failings and/or have no mechanisms for allowing human attempts to correct inappropriate actions or inaccurate data. In order to deal with such problems, recent European legislation has decreed that data can only be used for the purposes for which it was collected. This is clearly in the data subject's interests, but how can the subject be reassured that it is being enforced?

These examples can all be seen as design issues. Can we

anticipate bad consequences in the human system which arise from the computer performing according to its specification rather than according to what is intended? And if we could, how would this affect the design process?

There are three components to the workshop. Firstly, a couple of invited papers will set the scene for discussing how social and ethical issues can be translated into design. Secondly, submitted papers have been chosen to reflect how some of the process and design problems can be addressed by system designers. Plenty of time has been allowed for discussion of the papers. Finally, a couple of debates will be arranged to give participants a chance to express their views on the extent to which social concerns demand trade-offs against efficiency (both process and product efficiency) and on how the designer strikes a balance between ethical considerations and the achievement of organisational objectives.

Invited Speakers are:

John Nicholls, University of Oxford: 'Design for protecting the user'.

M. Cavanagh: 'Ethics and system design'.

Other papers are by leading researchers from Europe, USA, and Australia.

They are grouped into four Sessions:

- 1: The Requirements Process
- 2: Regulatory Issues
- 3: Safety-critical Issues
- 4: Social Issues
- 5: Privacy Issues

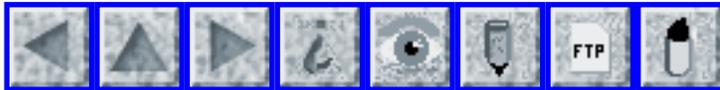
REGISTRATION AND INFORMATION

For further information about the programme, the delightful venue,
and how to register, please see the WWW pages given above, or
contact:

Mrs Carol Barrett
Centre Manager
Centre for Software Reliability
The City University
Northampton Square
London
EC1V OHB

Tel: +44 171 477 8421
Fax: +44 171 477 8585
e.mail: c.barrett@csr.city.ac.uk

The workshop is residential, and the full workshop registration
package is
UK Pounds 895. A specially reduced registration of UK Pounds
825 is
available to academics.



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 18: Issue 28

Thursday 26 July 1996

Contents

- [Johannesburg Stock Exchange Computer Fails, Again](#)
[Scott Hazelhurst](#)
- [Static Klingons and Dynamic Cash](#)
[Peter Wayner](#)
- [Sweden will not set limits for electric and magnetic fields](#)
[Martin Minow](#)
- [Cleaning person inadvertently kills patients](#)
[Archie Russel via Michael D. Crawford](#)
- [DMV security code breached at hospital in New Haven](#)
[Ed Fischer](#)
- [Risks of Using VISA Cash in Atlanta](#)
[Heather Hinton](#)
- [Computer systems and the Olympic Games](#)
[Jose Reynaldo A. Setti](#)
- [Esoteric Encryption Risks](#)
[Russ Broomell](#)
- [More on the Ariane-5 Disaster](#)
[Jan-Peter Munk](#)
- [Re: Western power outages](#)
[Mark Stalzer](#)

[Paul Green](#)

● [Re: the complexity of everyday life](#)

[Scot E. Wilcoxon](#)

[Bryan O'Sullivan](#)

● [Info on RISKS \(comp.risks\)](#)

✶ Johannesburg Stock Exchange Computer Fails, Again

Scott Hazelhurst <scott@concave.cs.wits.ac.za>

Wed, 24 Jul 1996 14:52:07 GMT

On 22 Jul 1996, the Johannesburg Stock Exchange's automated trading system, JET, failed for the second time this month (*) (Source: *Johannesburg's Business Day* newspaper of 23 July). Fully automated trading only started on 10 June.

After only forty minutes trading, the system failed as did the backup system, and did not come up again that day. Only R56m worth of trade was done, versus the average daily trade of R400m (R4.4 = US\$1).

Brokers complained of three negative consequences of this:

- the loss of margins on trade (although that would be partially offset by greater trades the next day)
- leaving many positions open for extended periods at a time of great stock market volatility both nationally and internationally
- loss of foreign investment confidence in the JSE (**)

Business Day of 24 Jul 1996 quoted the president of the JSE as saying that problems had been fixed and that there were no problems in trade on the

23rd. He described the error as an "an obscure network bug in the special coding written for the decentralised SA network". (***)

Comment:

* The first failure, on 1 July, was attributed to "human error".

** The article said that the system was supplied by the Chicago Stock

Exchange, and that it had been fixed by "technicians from the Chicago Stock Exchange". I would have thought that this would cause investors to worry more about the Chicago Stock Exchange.

*** I wonder what a non-obscure bug would be, if an obscure one stops trading on a large stock exchange (13th by market capitalisation, I believe) for almost a full day.

Hopefully all of this will help our Dependable Computing group raise funds from industry.

Scott Hazelhurst, Dept. of Computer Science, University of the Witwatersrand,
Johannesburg, 2050 Wits, South Africa +27 11 716-3806
scott@cs.wits.ac.za

Static Klingons and Dynamic Cash

Peter Wayner <pcw@access.digex.net>

Wed, 24 Jul 1996 18:34:35 -0400

Devoted and casual RISKS readers will both want to dig up the 24 Jul 1996

edition of the **Wall Street Journal**, which has two very important stories

on the front page. The first is a followup to the digital cash

heist where about one half a billion dollars disappeared through counterfeit cards used in Japanese Pachinko parlors. The story notes that the idea to use cards could be traced to a CIA briefing that suggested that the North Korean government was building nuclear weapons with money laundered through pachinko parlors controlled by Koreans living in Japan. The cards were supposed to bring accountability and traceability. Instead billions of yen disappeared. The article leaves the impression that the money ended up in Korea, although no one can really be sure of anything except that it is gone from the balance sheets of the corporations that developed the cards.

The second article describes how static electricity is beginning to be a real problem. The opening image comes from a room where the votes on a new tax levy were being tallied by computer. The first run of the computer showed the new tax being rejected by the voters. OOOPS. A bit of anti-static magic fluid was spread around the computer and the second run showed the new tax passing much to the relief of the people in power. The article goes on to say other interesting things about static, leaving RISKS readers hanging: How do they *know* which is the correct count? I bet I can guess which choice ended up being official.

🔥 Sweden will not set limits for electric and magnetic fields

Martin Minow <minow@apple.com>

Tue, 23 Jul 1996 23:01:36 -0700

An article in the Swedish newspaper, *Svenska Dagbladet* (23 Jul 1996,

http://www.svd.se/svd/ettan/X0006_Grnsvrden.html) by Annika

Carlsson notes

that Sweden will not establish limits for electrical and magnetic fields.

Instead, the government has agreed on a "policy of watchfulness" (foersiktighetspolicy). The article notes that, when a choice is possible,

one should choose technical solutions that yield the lowest electrical and magnetic fields.

Lars-Eric Paulson, researcher at SSI (The National Radiation Protection

Institute) stated: "We lack necessary research. When we started working two

years ago, we thought that research would yield limiting values, but this

couldn't be accomplished." Research did determine, however that, among the

approximately 70 Swedish children that get leukemia every year [out of a

population of about 9 million], one case is due to large electric power

transmission lines. [Note: I'm unsure of the proper translation here. A

literal translation would use "depends on" where I wrote "is due to." This

would seem to be a rather strong statement.]

Furthermore, about ten people per year get cancer because of "wandering

currents." I.e., electric currents that choose a path different than what is

intended, thus causing a doubled electric field: partially from the

wandering current and partially from the electric wiring.

The lack of a national policy has led to different approaches.

For example, Solna, a suburb of Stockholm, choose to run a major electric transmission underground even though, as Lars-Eric Paulsson notes. this wasn't recommended on electric field suppression grounds. However, Solna chose the more expensive alternative because of social and psychological concern for the residents in the transmission line's path.

According to SSI, no other country has set limits for electric and magnetic fields. The value of 0.2 micro-Tesla has been used at times, but there is no evidence that more intense fields are dangerous.

[Please excuse my clumsy translation.]

Martin Minow, minow@apple.com (former resident of Solna)

✂ Cleaning person inadvertently kills patients

"Michael D. Crawford" <crawford@scruznet.com>

Wed, 24 Jul 1996 23:27:06 -0700

I don't know if this is true, but it sounds plausible.
[Similar cases have been reported previously in the RISKS archives.]

>>From: Archie Russell <archier@gulag.CS.Berkeley.EDU>

>>

>>"For several months, our nurses have been baffled to find a dead patient in

>>the same bed every Friday morning" a spokeswoman for the Pelonomi Hospital

>>(Free State, South Africa) told reporters. "There was no apparent cause for

>>any of the deaths, and extensive checks on the air conditioning system, and

>>a search for possible bacterial infection, failed to reveal any clues."
>>
>>"However, further inquiries have now revealed the cause of these deaths. It
>>seems that every Friday morning a cleaner would enter the ward, remove the
>>plug that powered the patient's life support system, plug her floor polisher
>>into the vacant socket, then go about her business. When she had finished
>>her chores, she would plug the life support machine back in and leave,
>>unaware that the patient was now dead. She could not, after all, hear the
>>screams and eventual death rattle over the whirring of her polisher.
>>
>>"We are sorry, and have sent a strong letter to the cleaner in question.
>>Further, the Free State Health and Welfare Department is arranging for an
>>electrician to fit an extra socket, so there should be no repetition of this
>>incident. The enquiry is now closed."
>>
>>from (Cape Times, 6/13/96)
>>BTW, the headline of the newspaper story was, "Cleaner Polishes Off
>>Patients."

Mike Crawford crawford@scruznet.com <http://www.scruznet.com/~crawford/>

DMV security code breached at hospital in New Haven

<EdFischer@aol.com>

Thu, 25 Jul 1996 09:47:40 -0400

A security employee at the Hospital of St. Raphael in New Haven apparently disclosed a security access code (password?) for telephone access to DMV records, supposedly to be used only to check records following accidents or car breakins on the hospital campus, but of course providing access to all DMV records. The access code should not have been disclosed, and the employee's code and all other hospital codes have been cancelled, pending review. [Source: *Hartford Courant*, 25 July 1996, PGN Abstracting]

Edward Fischer, Director, Information Systems, Post-Newsweek Stations, Inc.
3 Constitution Plaza, Hartford CT 06103 (860) 493-2522
ed@postnewsweek.com

⚡ Risks of Using VISA Cash in Atlanta

Heather Hinton <hhinton@mailhost.ee.ryerson.ca>
Thu, 25 Jul 1996 09:43:40 -0400 (EDT)

The following article was included in "The Globe and Mail", a Toronto, Canada newspaper on Monday, July 22 (p.1, Section C):

>From Neil A. Campbell of the Globe's Olympic staff: "In an effort to be on the cutting edge of the Games, one of my \$20 bills was exchanged last week for a \$20 VISA cash card. The Olympics are being used to hype this new product, which is basically an Interac card without the PIN number. Just about everybody in Atlanta is supposed to be accepting VISA cash cards but the \$20 card is unblemished because the only merchant who knew

anything
about it had a machine that wasn't working. Colleague Jan Wong
was able to
buy two coffees with her \$5 card. But VISA cash can't be
combined with real
cash, so she is currently wandering Atlanta searching for
something that
costs \$1.44, including tax, so she can kiss off VISA cash
forever."

from Heather Hinton, hhinton@ee.ryerson.ca

✶ More on computer systems and the Olympic Games

"Jose Reynaldo A. Setti" <setti@labtrans.stt.eesc.sc.usp.br>

Thu, 25 Jul 1996 09:52:39 -0200

Among all problems that are embarrassing the ACOG, some are
really funny, as
the *Toronto Globe and Mail* reports today:

Results were flowing faster yesterday, but the Info '96
database,
which is supposed to provide biographical information to
journalists
and others, was still shaky. Biographies of many famous
athletes,
including U.S. long jumper Carl Lewis, were unavailable, and
information on others was so poor as to call the whole system
into
question. Lisa Neuberger, a sailor who carried the flag for the
Virgin Islands at the opening ceremonies, is listed as being 95
years old. Sule Olaleye of Nigeria is the 125th-ranked table-
tennis
player in the world. It is no wonder he is so unaccomplished--
the
computer insists he is only 17 centimetres tall.

The risks of depending on computers is that they tend to make

you older,
shorter and probably fat and bald, too.

Dr. Jose Reynaldo Setti, Universidade de Sao Paulo, Dept. of
Transport
Engineering 13560-250 Av. Carlos Botelho, 1465, Sao Carlos, SP
Brazil

✶ Esoteric Encryption Risks

"-Broomell, Russ" <MARKETING/MARKETING/RUSS%Konica_Imaging@mcimail.com>
Thu, 25 Jul 96 09:43 EST

While I'm not an expert in encryption, I have been following the on-going discussions on increasing standards. It seems to me that there's a broader risk that we're ignoring. It really hit home the other night...

A friend and I were having dinner, and since he knows that I work with computers for a living, he asked what I thought about taking customer orders through his web site. He had heard something about credit cards not being secure and wanted to know what I thought. I made the mistake of asking him how he put handles computer security in general.

He says that he uses the internet to send new product designs and costs to and from his manufacturers. If he feels they are **really sensitive** he uses a disk compression program with password protection. Then, for large files, he has his **computer person** copy the files to a directory on his web site - and he e-mails the location and password to the intended recipient.

He **makes sure there's no link pointing to the file, so nobody can find it**

and then deletes it after the recipient has acknowledged receipt.

The risk here is obvious - the discussion of 100+ bit encryption is lost on this guy - he uses little or no encryption for data protection.

Although maybe we can find a lesson here, that anonymity is still the best policy.

✈ More on the Ariane-5 Disaster

Jan-Peter Munk <munk@DBresearch-berlin.de>

Wed, 24 Jul 1996 09:46:38 GMT

Today (24 Jul 1996) here in Berlin, the local newspaper *Der Tagesspiegel* published some facts from the final inquiry report about the Ariane-5 disaster on 4 Jun. This report was officially released on Tuesday, 23 Jul.

In accordance to the report the Ariane-5 crash was caused by a faulty software. 37 secs after lift-off no information about present position and course was available. The data was to be delivered by a redundant set of Inertial Reference Systems (IRS). But two of these platforms (subsystems) failed. This failure was not(!) considered by the test software which ran before the lift-off.

The official inquiry commission found out that the IRS was designed for the preceding model, Ariane-4. That's why on 4 June 1996 a function was called that was supposed to align the missing Inertial platforms. But: This

function was not necessary for Ariane-5! However, this alignment function overloaded the computer, and as a result, the necessary data was not delivered.

"This [design, JPM] fault could have been discovered", Mr. Wolfgang Kubbat (Darmstadt U of Technology) as a member of the inquiry commission was cited. The vice chairman of the commission, Mr. Lennart Luebeck, emphasized the demand for better and more realistic tests.

The president of the European Space Agency (ESA), Mr. Luton, said that there won't be a discussion on the system architecture [of Ariane-5, JPM]. He estimates a total cost rise for the program of about 2 to 4 percent (current state: 37 billion FF/ 11 billion DEM).

The next launch of a Ariane-5 is considered for spring 1997.

Jan-Peter Munk (student), Daimler-Benz AG, Research and Technology
Alt-Moabit 96a, D-10559 Berlin munk@DBresearch-berlin.de
JPMunk@t-online.de

[BTW, The brief quote cited in [RISKS-18.27](#) by Pat Lincoln was followed in the full text by this:

- > The extensive reviews and tests carried out during the Ariane
- > 5 development programme did not include adequate analysis and
- > testing of the inertial reference system or of the complete flight
- > control system, which could have detected the potential failure.

- > Despite the series of tests and reviews carried out under the

> programme, in the course of which thousands of corrections were
> made, shortcomings in the system approach concerning the
> software resulted in failure to detect the fault. It is stressed that
> alignment function of the inertial reference system, which served
> a purpose only before lift-off (but remained operative afterwards),
> was not taken into account in the simulations and that the
> equipment and system tests were not sufficiently representative.

<http://www.esrin.esa.it/htdocs/tidc/Press/Press96/press33.html>

PGN]

🔥 Re: Western power outages (Pettit, [RISKS-18.27](#))

Mark Stalzer <stalzer@macaw.hrl.hac.com>

Wed, 24 Jul 1996 10:16:22 -0700

Tracy Pettit wrote an interesting piece in [RISKS-18.27](#) on the US power grid and its vulnerabilities. I want to take issue with one point however, namely that setting electricity rates in a market will lower reliability. [...]

I think a market based approach might let us discover a better balance between cost and reliability. The bond market is a good analogy, the cost of US treasuries for a given rate is higher than corporate bonds since people are willing to pay more for the reliability of government bonds (please, no laughing). Similarly, many consumers of electricity (municipal

distributors)
will probably be willing to pay a bit more for power from a utility that has a good reliability record. Others might go after the cheapest power possible, even with outages, to perform tasks that are not time critical like pumping water into a reservoir or charging electric cars. You might get an increase in reliability if redundant networks of different grades of power start to appear. The overall impact on reliability is difficult to say, but it might actually improve.

Mark Stalzer, mas@acm.org

⚡ Re: Western power outages (Pettit, [RISKS-18.27](#))

<Paul_Green@vos.stratus.com>

Wed, 24 Jul 96 17:39 EDT

The Massachusetts Department of Public Utilities is currently undergoing a comment period regarding their proposed rulemaking on unbundling electric producers from transmission companies. If you act quickly you can get your comments submitted in a timely fashion.

The brochure they had inserted in my electric bill says "The CPU will work to ensure that the new system will be as safe and reliable as the current structure." Where I live (fairly rural town), I estimate that the electric service is about 99% reliable; i.e., about 8 hours downtime/year. Not so good. While most outages are fairly short (~1 hour), each year

we seem to
get a major outage (~6 hours). Thus, I own a rather large
generator, and I
do use it. It is my understanding that most of our outages are
transmission-related and are due to weather or motor vehicle
accidents.

The proposed rules are online at "[http://www.magnet.state.ma.us/
dpu/](http://www.magnet.state.ma.us/dpu/)".

The public comment period ends on August 2, 1996. The E-mail
address
for comments is: "dpuask@state.ma.us".

The postal address for comments is:
Mary Cottrell, Secretary
RE: DPU 96-100
Department of Public Utilities
100 Cambridge St
Boston, MA 02202 USA

Paul Green, Sr. Technical Consultant, Stratus Computer,
Marlboro, MA.

✉ Re: the complexity of everyday life (Norman on Tenner, [RISKS-18.27](#))

"Scot E. Wilcoxon" <sewilco@fieldday.mn.org>
Tue, 23 Jul 1996 22:58:15 -0500

>The main emphasis is on the unintended side effects of human
introduction
>of items alien to the culture or environment

Keep this in perspective. The complexity of everyday life in
developed
countries is much simpler than the complexity of everyday life
for Man in
the wild. Without our technology, we would spend a lot of time

fending off
our natural environment (including germs, lice, and predators)
and feeding
ourselves (hope for global temps to rise to normal so there's
more food and
more large animals to hunt).

Scot E. Wilcoxon sewilco@fieldday.mn.org

✦ **Re: the complexity of everyday life (Norman on Tenner, [RISKS-18.27](#))**

"Bryan O'Sullivan" <bos@serpentine.com>
Tue, 23 Jul 1996 17:45:54 -0700 (PDT)

RISKS of books about RISKS?

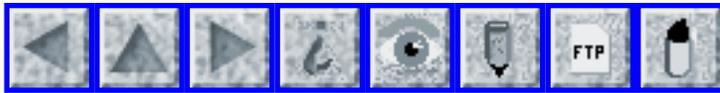
In [RISKS-18.27](#), Don Norman recommends Edward Tenner's "Why Things Bite Back" as a fine book on the unintended consequences of technology. While I am inclined to agree that it makes a diverting light read, I would not commend it for serious perusal.

As Caitlin Burke's review of this book (which may be found at <http://www.thenetnet.com/>) makes clear, Tenner is somewhat confused by his subject matter, and is prone to undermining his own points through the lightweight treatment he devotes to them. [Caitlin Burke <caitlinb@best.com>]

The most notable instance of this she cites is Tenner's coverage of Post-Traumatic Stress Disorder (PTSD). Tenner suggests that the improved ability of the military to treat wounded soldiers and return them to service

was a major factor the high incidence of PTSD, making no mention of much more important issues such as the nature of the training soldiers received, their youth, or disapproval of the war "back home".

While Tenner's proclivity towards undermining the ironies he seeks to expose through the introduction of unintended ironies of his own is unfortunate, his book is an enjoyable, and largely (even studiously) uncontroversial, romp. One final caution is, however, in order: "Why Things Bite Back" focuses much more on biological issues than on those relating to computers, and as such may not provide substantial grist for the mills of RISKS readers.



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 18: Issue 29

Wednesday 31 July 1996

Contents

- [Another Ruling Against Communications Decency Act](#)
[Edupage](#)
- [Bringing Design to Software, Terry Winograd](#)
[PGN](#)
- [Where Wizards Stay Up Late, Katie Hafner and Matthew Lyon](#)
[PGN](#)
- [Crisis management, National Research Council report](#)
[PGN](#)
- [Clinton Anti-Terrorism Plans Called Threat to Civil Liberties](#)
[Edupage](#)
- [Olympic bomb warning call](#)
[Steven Bellovin](#)
- [System Testing Begins When System Is Tested](#)
[Keith Farkas](#)
- [More on: Problems with Olympic Information System](#)
[Tom Rowe](#)
- [Y2K hits divorcing couples in the UK](#)
[Mike Hanafin](#)
- [Safety vs. money, always a problem](#)
[Geoff Kuenning](#)

- [Risks of electronic credit card operations](#)
[Robert Schwanke](#)
 - [Computers Causing Power Outages](#)
[D.C. Sessions](#)
 - [Re: Mark Stalzer and Western Outages](#)
[Phil Hammons](#)
 - [Re: Western power outages: Errata for RISK-18.28](#)
[Paul Green](#)
 - [Re: Cleaning person inadvertently kills patients](#)
[Prabhakar Ragde](#)
[Geoff Kuenning](#)
[Steve Kilbane](#)
 - [Ariane 5 failure - due to register overflow](#)
[Hans-Martin Adorf](#)
 - [Findings of the Ariane 501 inquiry board](#)
[Kristiansen](#)
 - [Info on RISK \(comp.risks\)](#)
-

⚡ Another Ruling Against Communications Decency Act

Edupage Editors <educom@elanor.oit.unc.edu>

Wed, 31 Jul 1996 11:11:37 -0400 (EDT)

Echoing a decision made last month by federal judges in Philadelphia, a three-person panel of federal judges in Manhattan rule the Communications Decency Act (part of the Telecommunications Act of 1996) to be unconstitutional. The Act makes it a felony to transmit "indecent" or "patently offensive" material over computer networks where children might have access to it. The law suit involved an Internet-based newsletter opposed to legislation banning indecent but constitutionally protected speech on the Internet. The newsletter's author says it was "laced with

four-letter and multisyllabic obscenities familiar to anyone and, frankly, the day I published that article, I had some very real fears of going to prison. But I felt so deeply that our rights were violated by the law, I had an obligation to fight it." The Justice Department is appealing the Philadelphia decision to the U.S. Supreme Court. (*The New York Times*, 30 Jul 1996, A7; Edupage, 30 Jul 1996)

✦ Bringing Design to Software, Terry Winograd

"Peter G. Neumann" <neumann@csl.sri.com>
Wed, 31 Jul 96 9:03:03 PDT

RISKS has since its inception 11 years ago (1 Aug 1985) noted the importance of up-front efforts in avoiding risks. Having sound requirements and a sound design tends to save great agonies further down the line. A new book provides a fascinating collection of chapters that present various different approaches to software design:

Bringing Design to Software
Terry Winograd (editor)
Addison-Wesley (Reading, Massachusetts)
and ACM Press Books (New York)
1996
ISBN 0-201-85491-0

Although the topics are intentionally quite diverse, there seems to be something useful for everybody. Chapter contributors include Mitch Kapor, David Liddle, Gillian Crampton Smith and Philip Tabor, John

Rheinfrank and
Shelley Evenson, Paul Saffo, Peter Denning and Pamela Dargan,
John Seely
Brown and Paul Duguid, David Kelley and Bradley Hartfield,
Donald Schon and
John Bennett, Michael Schrage, Shahaf Gal, Donald Norman, Laura
De Young,
and Sara Kuhn.

🔥 Where Wizards Stay Up Late, Katie Hafner and Matthew Lyon

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

Wed, 31 Jul 96 9:52:18 PDT

Where Wizards Stay Up Late: The Origins of the Internet
Katie Hafner and Matthew Lyon
Simon and Schuster, New York, NY
1996
ISBN 0-684-81201-0

At first glance, this new book might not seem sufficiently risks related for me to comment on it here. However, one of the biggest risks involving many people in computer-related fields seems to be a lack of a sense of history -- except for a few old-timers such as me (but we forget!) and a few younger folks who have assiduously tried to study the past (except that it is usually not well documented). The RISKS archives strongly suggest that the same kinds of problems keep recurring, and that knowledge of the past can help significantly to avoid those risks in the future.

This book will make fascinating reading for those of you who don't know the early history of the ARPAnet. It points out how only a very few people and

almost no corporations foresaw the incredible potential of the emerging networking technology. The book details how the network evolved nevertheless -- primarily because of the tremendous energies and visions of a few farsighted people.

Let me add an editorial note. With its emphasis on advances in connectivity (for example, packet switching, high availability, alternative routing, and scalability), there was quite consciously very little emphasis on network security in the early ARPAnet days -- and not enough emphasis on host-system security. You might think that is coming back to haunt us now, with all the security flakiness relating to the Internet. However, confidentiality can be enforced by the use of end-to-end cryptography, and authentication is a natural burden of the hosts anyway, so the burden falls more strongly on the operating systems. Nevertheless, prevention of denials of service is still in part a networking problem -- although we certainly don't need attacks in order to have performance degradations! Recently, while in Massachusetts, I had repeated serious problems with network reliability telnetting back to California. On one occasion, I discovered that two of the major transcontinental nodes on which I had to depend were *each* dropping about 40% of their packets, over a prolonged period of time. Perhaps the real problem is that the wizards are no longer staying up late enough, or that the new quasiwizards are not familiar enough with history and the sense of accomplishment that prevailed in the ARPAnet days. Mayhaps this book will help.

✂ Crisis management, National Research Council report

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

Tue, 30 Jul 96 11:57:51 PDT

Computing and Communications in the Extreme:

Research for Crisis Management and Other Applications
Computer Science and Telecommunications Board,
National Research Council,
National Academy Press, 1996

The full text is available <<http://www.nap.edu/readingroom/books/extreme>>.

This book is the results of ongoing investigations of the Workshop Series on High-Performance Computing and Communication. The steering committee was chaired by Ken Kennedy of Rice University, and included Frances Allen, Vint Cert, Geoffrey Fox, Bill Scherlis, Burton Smith, and Karen Sollins.

✂ Clinton Anti-Terrorism Plans Called Threat to Civil Liberties

Edupage Editors <educom@elanor.oit.unc.edu>

Wed, 31 Jul 1996 11:11:37 -0400 (EDT)

To fight terrorism, the Clinton administration is proposing a number of measures which civil libertarians say pose a serious threat to the freedoms of innocent users of phones and computers. A spokesman for the American

Civil Liberties Union says: 'The president is using the bombing in Atlanta as a pretense to getting more wiretap authority. The answer to terrorism isn't to limit the freedoms of Americans. If we do that, the terrorists have already won.' (*San Jose Mercury News*, 30 Jul 96; Edupage 30 July 1996)

🔥 Olympic bomb warning call

Steven Bellovin <smb@research.att.com>

Tue, 30 Jul 1996 12:33:43 -0400

Before the bomb exploded at Centennial Olympic Park in Atlanta, there was a call to the 911 emergency number warning of it. But there was a 10 minute lag between when the call was received and when a police officer was dispatched. Why? According to the Associated Press, the dispatchers needed a street address for the park because the computer system they're using requires one in order to transmit the information.

[Also noted by Sean Smith <sean@c3serve.c3.lanl.gov>. PGN]

🔥 System Testing Begins When System Is Tested (Edupage, IBM Olympics)

Keith Farkas <farkas@eecg.toronto.edu>

Sat, 27 Jul 1996 11:36:06 -0400

Complaining about the computer system that failed in the opening days of the

Olympics to provide timely and accurate information about competitive events, journalists asked Billy Payne, the president of the Atlanta Olympics Organizing Committee, "Why wasn't the technology system tested?" Payne replied that "there is no way to duplicate the totality of the Olympic condition before the start of the games." [Source: Edupage, 25 July 1996, quoting *Atlanta Journal-Constitution* Olympic City p34]

[I was told yesterday during a panel session at the WICS summer course on Internet Security at Stanford that the system is no longer Olymping along, and that everything seems to be working well now. I haven't tried it myself. PGN]

⚡ More on: Problems with Olympic Information System

<<Tom.Rowe@news.doit.wisc.edu> trowe@aae.wisc.edu>
29 Jul 1996 15:33:56 GMT

IBM stated that typically they need 30-60 (or 60-90, I forget which) days to set up the type of networking systems used in Atlanta that journalists are complaining about. In many cases they had 2-3 days because of delays in the committee deciding on venues. I don't know who took the most foolish risk, the games committee for giving so little time for such a complicated system, or IBM for accepting such restrictive conditions. Tom Rowe UW-Madison

⚡ Y2K hits divorcing couples in the UK

Mike Hanafin <hanafinm@glas.cork.rtsg.mot.com>

Tue, 30 Jul 1996 12:19:48 +0100

Yet another example of our impending millenium change causing trouble.

This time ordinary people, rather than companies, are directly affected.

>From the *Electronic Telegraph* of 30 Jul 1996:

> PLANS to split the pensions of divorcing couples have been delayed
> until the next century because of problems with the Department of Social
> Security computer, the Government admitted yesterday. ...
> Although the Government sees the need for a change in the law to give
> partners equal rights to pensions, he said the new legislation would not
> be implemented until after 2000 because a big shake-up of the database
> of National Insurance numbers was now underway."

The RISK is: How many more government databases worldwide will be affected by Y2K? And if more are, do they realise it and are they actively working on fixing the problem? They may not always be able to legislate around this issue.

Mike Hanafin Motorola Cork, Ireland hanafinm@cork.cig.mot.com

⚡ Safety vs. money, always a problem

Geoff Kuenning <geoff@ficus.cs.ucla.edu>

Tue, 30 Jul 1996 10:46:58 -0700

I heard an advertisement on the radio the other day which highlights one of the difficulties we face in designing reliable, safe systems. The announcer touted a new feature on BMW automobiles which detects whether a passenger is present. This information is used to suppress deployment of the passenger-side airbag in accidents when appropriate. The reason for the feature, and the point made by the ad, is that replacing an airbag costs about \$2500 (actually, they quoted the price for a competitor, not their own car). So why inflate the bag if there's nobody to be saved?

RISKS readers are probably shuddering at this concept. A well-designed failsafe system would err on the side of unnecessary deployment, not saving a few dollars. One would hope that the passenger sensor is designed to fail into the "passenger present" mode, but it is difficult to imagine a technology which could be guaranteed to do so in all cases. The fundamental problem is that the detection subsystem is designed to suppress a safety-related behavior in the main system, rather than to redundantly encourage it, all to save money. This makes the entire system dependent on the correct operation of the subsystem.

I cannot help suspecting that a few years from now, when the passenger sensors and wiring begin to wear out, BMW will suffer some lawsuits because passenger airbags should have deployed, but didn't.

Geoff Kuenning g.kuenning@ieee.org geoff@ITcorp.com
<http://fmg-www.cs.ucla.edu/geoff/>

⚡ Risks of electronic credit card operations

Robert Schwanke <rws@scr.siemens.com>

Wed, 31 Jul 1996 11:15:49 -0400 (EDT)

I just went through an amusing process of trying to pay my son's college tuition by credit card. The university provided the authorization form by which to do it, and it has worked in previous semesters.

However, I got a phone call from the university cashier, saying the charge was declined by the bank.

I called the bank, and was told that the charge was declined because it was over \$5000. As a security precaution, they expect the cashier to phone in for a verbal authorization. They marked my account with my verbal OK, and said the cashier could phone them directly for a verbal authorization.

I called the cashier back. She said she can't do anything unless her computer calls her bank, her bank calls my bank, and my bank okays the transaction. I asked her if I could give her my bank's phone number so she could call and find out what's going on. She said sure.

She called back later and left a message saying the charge had been declined again. I called my bank to see if she had called them, and they said no, it would have been noted on my account records. They explained that the cashier probably had no procedure for handling a verbal

authorization; that
many places can no longer do it "the old-fashioned way". But
they would
call her themselves and try to make it happen.

They called the cashier, who had left for the day, but left a
message with
another cashier giving the authorization code.

The next day the cashier called me again to tell me that the
charge was
still being declined. I asked if she had called my bank. She
said she had
given my bank's number to her bank, and they had promised to
call. They had
called her back to say that the charge had been declined.

I said, okay, let's split it into two transactions. Please put
the first
one through for \$4999. Okay, she said, that went through. I
said, okay,
now put through a second transaction for the balance. Okay, she
said, that
went through, too.

So much for security.

Robert.Schwanke@scr.siemens.com rws@scr.siemens.com (609) 734-
6546 Fax -6565
Siemens Corporate Research, Inc., 755 College Rd. East,
Princeton, NJ 08540

Computers Causing Power Outages

"D.C. Sessions" <dc.sessions@tempe.vlsi.com>
Tue, 30 Jul 1996 09:34:44 -0700

Every year we add to the "intelligence" of our electrical
appliances,

notably computers but also more mundane items such as microwave ovens, air conditioners, microwave (yup!) clothes dryers, etc. Requirements such as power-factor correction accelerate this trend. As a result, the electrical distribution load net is slowly shifting from a constant-impedance line (electric light) to a constant-power line (computer power supplies).

The RISK? Constant-power loads exhibit negative resistance: as the voltage drops, the current **increases**. As a result, the old-fashioned 'brownout' is a thing of the past. The electrical distribution network is becoming more and more unstable. Currently it's only unstable at the low-voltage end of the supply curve, but eventually the instability will reach normal operating levels.

I got a taste of this in an industrial-automation system a while ago. If you think the Year 2000 problem is going to be fun, just **imagine** trying to manage the power-distribution network in a few years.

D. C. Sessions dc.sessions@tempe.vlsi.com

⚡ Re: Mark Stalzer and Western Outages

"Hammons, Phil" <HAMMONSP@msl.aes.com>
Mon, 29 Jul 96 10:49:00 -

I wonder where Mark lives to develop the model he is using. Living in the west where we can see several problems with his model from the front door.

1. To use an economic model to describe a physical entity is at best unwise and mostly worthless. The only legitimate comparison is that Government agencies are involved in both and neither is well respected (which has nothing to do with reliability).

2. He speaks of Redundant Networks of different grades of service. Two issues:

A. In a world where it takes multiple organisations to build one grid,

Where do we find the organizations to build these additional grids?

B. In the WEST, where do we find the redundant paths for these grids

without destroying the environment that many of us came west for?

3. In your competitive model, who fixes the following situation which is

necessary and too, too common. A young lady goes to visit a friend living in

a hillside home. After the visit, she loses control of her van and crashes

the power pole that supplies power to my house (among many others). Power to

our neighborhood is out for 17 hours. The pole must be replaced, crews work

all night, and service is finally restored. Who's going to do the job in

your model? This is real life, last Friday to be exact.

✉ Re: Western power outages: Errata for [RISKS-18.28](#)

<Paul_Green@vos.stratus.com>

Fri, 26 Jul 96 13:07 EDT

The abbreviation "CPU" should read "DPU". 8 hours downtime per year is about 99.9% reliable, not 99% as I had said. My thanks to Dr. Marty Ryba of MIT for catching this.

Paul Green, Stratus Computer

["DPU" corrected in SRI archive copy. PGN]

✂ Re: Cleaning person inadvertently kills patients ([RISKS-18.28](#))

Prabhakar Ragde <plragde@plg.uwaterloo.ca>

Fri, 26 Jul 1996 10:55:01 -0400 (EDT)

Mike Crawford submitted in [RISKS-18.28](#) an apparently doubly-forwarded item about a cleaner in a South African hospital unplugging a life-support system every Friday to plug in her floor polisher. I found the news item on the Web site of the Cape Times. It was changed considerably by the time of its appearance in RISKS: somewhere along the line, implausible bits about the "screams and death rattle" of the victims and about a hospital spokesperson "sending a strong letter to the cleaner" was added. The original said only that a hospital spokesperson denied knowledge of the incident, and that only one of the deaths (all of which happened two years ago) was under investigation by the Free State Health and Welfare Department.

The item was also at an odd location in the Independent Online Webspaces:

http://www.inc.co.za/online/news/editorial/film_reviews/topmovies.html.

I'm dubious.

Prabhakar Ragde, Department of Computer Science, Univ. Waterloo,

Waterloo,
Ontario CANADA N2L 3G1 (519)888-4567,x4660 <http://plg.uwaterloo.ca/~plragde>

✶ Re: Cleaning person inadvertently kills patients ([RISKS-18.28](#))

Geoff Kuenning <geoff@ficus.cs.ucla.edu>

Thu, 25 Jul 1996 15:56:14 -0700

Michael D. Crawford writes:

> I don't know if this is true, but it sounds plausible.

It has the ring of urban legend to me. If a hospital was losing people every Friday, don't you think they would fairly quickly set up a watch on that bed? Also, if the deaths had really happened and the mistake admitted as readily as quoted, one suspects that there would be lots of news stories about the subsequent lawsuits.

Geoff Kuenning g.kuenning@ieee.org <http://fmg-www.cs.ucla.edu/geoff/>

✶ Re: Cleaning person inadvertently kills patients ([RISKS-18.28](#))

<Steve_Kilbane@cegelecproj.co.uk>

Fri, 26 Jul 1996 08:41:54 +0100

> I don't know if this is true, but it sounds plausible.
> [Similar cases have been reported previously in the RISKS archives.]

Oh, it happens, although not necessarily with such consequences.
I happened
to be in the office recently unplugged the UNIX box next to mine
in order to
plug the vacuum in. "Oh, did I unplug something?" she asked, in
apparent
surprise. Gurgle. Are there really places that put power cables
into
sockets, just to keep the sockets free of dust, or what?

steve

✶ Ariane 5 failure - due to register overflow

Hans-Martin Adorf <adorf@eso.org>
Mon, 29 Jul 1996 12:37:12 +0200

Excerpt from <http://sspg1.bnsc.rl.ac.uk/Share/ISTP/ariane5rep.htm>

[...]

The launcher started to disintegrate at about H0 + 39 seconds
because of
high aerodynamic loads due to an angle of attack of more than 20
degrees
that led to separation of the boosters from the main stage, in
turn
triggering the self-destruct system of the launcher.

This angle of attack was caused by full nozzle deflections of
the solid
boosters and the Vulcain main engine.

These nozzle deflections were commanded by the On-Board Computer
(OBC)
software on the basis of data transmitted by the active Inertial
Reference System (SRI 2). Part of these data at that time did not
contain proper flight data, but
showed a diagnostic bit pattern of the computer of the SRI 2,

which was interpreted as flight data.

The reason why the active SRI 2 did not send correct attitude data was that the unit had declared a failure due to a software exception.

The OBC could not switch to the back-up SRI 1 because that unit had already ceased to function during the previous data cycle (72 milliseconds period) for the same reason as SRI 2.

The internal SRI software exception was caused during execution of a data conversion from 64-bit floating point to 16-bit signed integer value. The floating point number which was converted had a value greater than what could be represented by a 16-bit signed integer. This resulted in an Operand Error. The data conversion instructions (in Ada code) were not protected from causing an Operand Error, although other conversions of comparable variables in the same place in the code were protected. [...]

✶ Findings of the Ariane 501 inquiry board

Kristiansen <ekristia@xs4all.nl>

Sat, 27 Jul 1996 21:45:28 +0200 (MET DST)

The inquiry board investigating the loss of the first Ariane 5 launcher has presented its conclusions. I have not seen the actual report of the board, but I have access to an official summary. Even the summary is a rather lengthy document, so I have extracted the parts which directly concern the

sequence of events, and the causes of the failure. The extracts are verbatim, except for my possible typos.

- During the launch preparations and the count-down no events occurred which were related to the failure. The meteorological conditions were acceptable, and no other external factors have been found to be of relevance.

- At 36.7 seconds after H0 (approx. 30 seconds after lift-off) the computer within the back-up inertial reference system, which was working on stand-by for guidance and attitude control, became inoperative. This was caused by an internal variable related to the horizontal velocity of the launcher exceeding a limit which existed in the software of this computer.

- Approx. 0.05 seconds later the active inertial reference system, identical to the back-up system in hardware and software, failed for the same reason. Since the back-up inertial system was already inoperative, correct guidance and attitude information could no longer be obtained and loss of the mission was inevitable.

- As a result of its failure, the active inertial reference system transmitted essentially diagnostic information to the launcher's main computer, where it was interpreted as flight data and used for flight control calculations.

- On the basis of those calculations, the main computer commanded the booster nozzles, and somewhat later the main engine nozzles also, to make a large correction for an attitude deviation that had not occurred.

- A rapid change of attitude occurred which caused the launcher to disintegrate at 39 seconds after H0 due to aerodynamic forces.
- Destruction was automatically initiated upon disintegration, as designed, at an altitude of 4 km and a distance of 1 km from the launch pad.
- The inertial system of Ariane 5 is essentially common to a system which is presently flying on Ariane 4. The part of the software which caused the interruption in the inertial system computers is used before launch to align the inertial reference system and, in Ariane 4, also to enable a rapid realignment of the system in case of a late hold in the countdown. The realignment function, which does not serve any purpose on Ariane 5, was nevertheless retained for commonality reasons and allowed, as in Ariane 4, to operate for approx. 40 seconds after lift-off.
- During design of the software of the inertial reference system used for Ariane 4 and Ariane 5, a decision was taken that it was not necessary to protect the inertial system computer from being made inoperative by an excessive value of the variable related to the horizontal velocity, a protection which was provided for several other variables of the alignment software. When taking this design decision, it was not analyzed or fully understood which values this particular variable might assume when the alignment software was allowed to operate after lift-off.
- In Ariane 4 flights using the same type of inertial reference

system there has been no such failure because the trajectory during the first 40 seconds of flight is such that the particular variable related to horizontal velocity cannot reach, with an adequate operational margin, a value beyond the limit present in the software.

- Ariane 5 has a high initial acceleration and a trajectory which leads to a build-up of horizontal velocity which is five times more rapid than for Ariane 4. The higher horizontal velocity of Ariane 5 generated, within the 40-second timeframe, the excessive value which caused the inertial system to cease operation.

- The specification of the inertial reference system and the tests performed at equipment level did not specifically include the Ariane 5 trajectory data. Consequently the realignment function was not tested under simulated Ariane 5 flight conditions, and the design error was not discovered.

- Post-flight simulations have been carried out on a computer with software of the inertial reference system and with a simulated environment, including the actual trajectory data from the Ariane 501 flight. These simulations have faithfully reproduced the chain of events leading to the failure of the inertial reference systems.



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 18: Issue 30

Thursday 8 August 1996

Contents

- [America Off-Line](#)
[PGN](#)
- [AOL outage: risks of scaling inappropriately](#)
[Joel M Snyder](#)
- [Trains fail to trigger computerized crossing gates](#)
[Mark Brader](#)
- [The Crash Detectives: USAir Flight 427](#)
[Jonathan Harr in the *New Yorker*](#)
- [A bug in the zipcode-catalog](#)
[Martin Minow](#)
- [Occam's Razor debunked](#)
[David Bruce via Peter M. Weiss](#)
- [International Hacking Incident](#)
[Andrew Blyth](#)
- [New system blamed for missed payments](#)
[David Kennedy](#)
- [Kirk Enterprises: What's in a name?](#)
[Andrew Koenig](#)
- [The increasing complexity of everyday life](#)
[Rshek](#)

- [Department of Motor Vehicle records available On-Line](#)
[Rich Ellermeier](#)
 - ["Anonymous" phone tips and Calling Number Identification](#)
[Michael Cook](#)
 - [Re: Where Wizards Stay Up Late](#)
[Danny Cohen](#)
 - [Re: IBM's Olympic Systems](#)
[Dave Wortman](#)
 - [Re: Computers causing power outages](#)
[Paul Peters](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ America Off-Line

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

Thu, 8 Aug 96 8:34:26 PDT

America Online's computer systems (near the Dulles Airport facility in Virginia) went down at 4am EDT on 7 Aug 1996. Service was reportedly restored sporadically 19 hours later, around 11pm EDT. The crash was caused by new software installed during a scheduled maintenance update. The 16 million people affected will apparently be given a free day of service (hopefully in addition to yesterday!). (AOL noted that this problem was different from their one-hour outage on 19 June 1996.)

* ``It's another reminder of how close to the edge a lot of these systems are,' ' said Richard Zwetchkenbaum (International Data Corp)...

[No news to RISKS readers]

According to David Einstein (*San Francisco Chronicle*, 8 Aug 1996, p.A1),

AOL officials have bragged about the reliability of their system. In fact, earlier this week one representative told The Chronicle that AOL computers are ``virtually immune'' to this kind of outage. [Virtual immunity is no virtue?]

[Outage also noted by David Kennedy <76702.3557@CompuServe.COM>.]

⚡ AOL outage: risks of scaling inappropriately

"Joel M Snyder, Now Overwhelmed Again" <Joel_M_Snyder@Opus1.COM>
Thu, 08 Aug 1996 08:33:30 -0700 (MST)

The repercussions of this were felt a long way away from AOL.

One of my clients is a public organization which sends out tens of thousands of messages a day advising people on the current status of pending legislation. People are encouraged to subscribe to this free service to follow their favorite bills.

Yesterday morning, I got a call because their mail system was backing up heavily. It took a while to discover the cause, but it turned out to be AOL. Because AOL's incoming mail from the Internet runs on relatively slow systems, and because they receive hundreds of thousands of Internet messages a day, they have 30 systems to receive incoming mail, all pointed at from the AOL.COM name. That means that any mail system trying to send mail to AOL would have to individually try all 30 addresses before

giving up. Translate that to a 60 second (typical) wait for a connection timeout, and you've got a 30 minute time-in-queue for an AOL message.

Well, this client was using multi-threaded mailers, but because of AOL's massive presence on the Internet & the large number of messages addressed to them, AOL messages ended up clogging up all of the outgoing queue spots. Hundreds of them.

The solution, unfortunately, is to treat AOL mail separately from other Internet mail. It now gets its own queue and is specifically segregated away from other mail so that this doesn't impact other users. The downside of this is that ALL AOL mail is now operated (implicitly) at a lower priority than other Internet mail, which means that AOL users have effectively become second-class citizens.

The risk? While growing so large (and having all your eggs in one basket) offers tremendous economies of scale, it has other exogenous effects. We are already familiar with the implicit social reaction that AOL's marketing strategy has brought on all their users from some corners of the Internet: "oh you're from AOL, you must be clueless," a sort of techno-racism aimed at the profile of the typical AOL user. Now, AOL's size may cause their users other discrimination of a more technical nature.

Joel M Snyder, 1404 East Lind Road, Tucson, AZ, 85719 +1 520 324 0494 (voice)
+1 520 324 0495 (FAX) jms@Opus1.COM <http://www.opus1.com/jms>

⚡ Trains fail to trigger computerized crossing gates

<msb@sq.com>

Tue, 6 Aug 96 16:14:29 EDT

A recent posting in misc.transport.urban-transit cites a 3 Aug 1996 article in **Newsday**, the major newspaper of Long Island, NY.

The Long Island Rail Road, a commuter railway connecting New York to the Long Island suburbs, recently tested three level crossings after a train passed one of them and its driver noticed that the gates did not operate. The three crossings, all in a place called Sayville, each "use the same microprocessor" and are the only ones on the LIRR to do so. The failure proved to be reproducible at two out of the three.

This would make me wonder about the third one, not to mention level crossings on other railways where the same hardware may be in use. (For instance, if the problem is a bug in the programming, it might well be one that comes and goes quasi-randomly. Of course, it might also be a failure any of several other sorts.) As a short-term measure, the LIRR stationed their police at each of the three crossings.

The LIRR also suffered similar problems last year, but says that the two cases are "apparently unconnected".

I don't know why the crossing gate needs a microprocessor. One possible reason would be if trains regularly travel on that part of the

line at
widely differing speeds; then the crossing gates could be
lowered at the
same time interval in front of a faster or a slower train.

Mark Brader msb@sq.com SoftQuad Inc., Toronto

✂ The Crash Detectives: USAir Flight 427

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

Fri, 2 Aug 96 16:21:47 PDT

Jonathan Harr has a fascinating article (**The New Yorker**, 5 Aug 1996) on
the process of trying to unravel the still unexplained crash of
USAir flight
427, a Boeing 737, on approach to Pittsburgh on 8 Sep 1994. The
discussion
seems timely in the light of the recent TWA 800 disaster,

✂ A bug in the zipcode-catalog

Martin Minow <minow@apple.com>

Wed, 31 Jul 1996 17:00:22 -0700

>From the Swedish newspaper, Svenska Dagbladet, 1 Aug 1996,
reported
by Nils-Olov Ollevik.

http://www.svd.se/svd/ettan/X0002_Bugg.html

An incorrect comma [Sweden uses commas to separate integer and
fraction,
where the USA uses a period] can cause problems, especially when
dealing
with billing and accounting. The other day, a businessman was

about to
send an invoice to one of its customers and, at the last minute,
discovered
that the computer wrote an invoice for 1.5 million kroner
instead of the
150,000 that he intended.

The analysis determined that the CD version of the Swedish
postnumber
(zipcode) catalog contains a programming error -- a bug -- that
can modify
certain programs that are already loaded into the computer.
This affects
the popular administrative programs from from Scandinavian PC
Systems, SPCS,
in Vaxjo [Sweden].

"As far as I know, only the SPCS-programs are affected, but this
is
unacceptable no matter how large or small the problem is"
according to
product manager Jan Hultgren from the Swedish Post Office, who is
responsible for the catalog. ... The error is in the way the CD
program
handles installation in the Windows operating system. It would
be strange if
only our program was affected.

According to Jonas Svensson of SPCS, the post office program
automatically
changes Windows installations, such as the placement of commas
together with
digits. "The error is easy to fix as long as you are aware of
it," said
Svensson.

.. The Post Office sold about 100,000 copies of the CD-catalog.

Translated (quickly) by

Martin Minow, minow@apple.com

Occam's Razor debunked

"Peter M. Weiss +1 814 863 1843" <PMW1@PSUVM.PSU.EDU>

Sat, 3 Aug 96 09:44 EDT

QUADNET, 2 AUG 1996

RAZOR THEORY LEFT IN SHREDS

A Deakin University academic has cast new light on a basic philosophical and scientific problem that has been subject to debate for more than 2000 years.

And this has thrown doubt on the accuracy of many data analysis techniques commonly used in business computing.

"Occam's razor, a principle dating back at least as far as Aristotle, suggests that we should accept the simplest explanation consistent with all the known facts. This previously untested principle is widely used in current scientific practice," said Dr Geoff Webb, of Deakin's School of Computing and Mathematics in Australia.

Dr Webb has put this principle to the test, and found it wanting.

Occam's razor is a guiding principle in computers known as machine learning systems, a form of artificial intelligence. Tasks commonly employed in machine learning cover such diverse areas as medical diagnosis and identification of glass fragments collected at the scene of an accident.

Dr Webb's research has found that when put into practice Occam's razor doesn't work. "The results are clear cut: Occam's razor is worse than blunt,

it is truly disposable," he said.

To test the theory, Dr Webb modified a widely used machine learning system that uses Occam's razor combined with a principle based on the assumption of similarity. The modified version of the system abandoned Occam's razor and relied solely on the principle of similarity. The theories developed by the modified system were more accurate than the version that used Occam's razor.

Among the many users of machine learning systems are a new wave of computer scientists calling themselves "data miners". These scientists use machine learning systems based on Occam's razor to extract information from vast quantities of data.

Data miners are employed by retailers to identify new customers; the taxation office to identify tax fraud; by banks to help decide who should receive loans; by stock brokers to select investments; and recently by astronomers to identify 16 new quasars.

"Data mining seeks to extract information from data. By using Occam's razor, data miners are potentially missing much of the information in the data. That translates directly into missed business opportunities," Dr Webb warns.

"Occam's razor guides the user to look for simple explanations. But what good are simple explanations of a complex world?" he said.

Dr Geoff Webb can be contacted on webb@deakin.edu.au

Issued by:

David Bruce, Media Manager, Deakin University, Australia

Phone: 61 3 9244 5268 Email: db@deakin.edu.au

David Bruce, Communications, Deakin University - 1995 University of the Year

db@deakin.edu.au (03) 9244 5268 (03) 9822 1379 fax

✶ International Hacking Incident

Andrew Blyth <ajcblyth@glamorgan.ac.uk>

Mon, 5 Aug 1996 13:37:32 +0000

The following is taken from the **Sunday Times** (London, 4 Aug 1996):

American Intelligence agents have hacked into the computers of the European parliament and European commission as part of an international espionage campaign aimed at stealing economic and political secrets. The commission has called in security expert to block further American government agents spying on its workings.

Security officials have disclosed that they have discovered several instances in which its communications systems have been compromised by American hacking. They have also found evidence that the Americans have used information obtained by hacking to help in trade negotiations last year on the General Agreement on Tariffs and Trade (GATT).

The CIA has already been accused by the Japanese and the French governments if hacking into their communications networks in an attempt to obtain confidential trade secrets.

The European parliament computer network links together more than 5,000 computers, and it is used to private medical, financial and official government documents.

Dr Andrew Blyth, Department of Computer Studies, University of Glamorgan
Pontypridd Mid Glamorgan CF37 1DL, UK +44 1443 48 2245

⚡ New system blamed for missed payments

David Kennedy <76702.3557@CompuServe.COM>
31 Jul 96 15:27:10 EDT

[Courtesy of Associated Press via CompuServe's Executive News Service,
30 Jul 1996]

Missed Payments (By Catherine O'Brien, Associated Press Writer)

>> WASHINGTON (AP) -- Rep. John Dingell says the rent on his
>>district office was not paid one month. Rep. Ron Klink's phone
service
>>was nearly shut off because the bill was not paid by the House.
>> They and other House Democrats said Tuesday they were
embarrassed
>>that the government has missed some payments to businesses in
their
>>districts. And in this election year, they insisted that when
>>Democrats were in charge the checks went out on time.

<< DMK: Partisan sniping from both sides deleted >>

>> In June, the House's chief administrative officer, Scott
>>Faulkner, switched to a financial management system that
>>included new computer software. Klink said the change was made
>>despite a warning from Price Waterhouse that it would take two

>>years or more to get the House up and running on the new system.

o House members are each checking with their offices to see that various accounts have been paid or are outstanding.

Dave Kennedy [CISSP] InfoSec Recon Team Chief, National Computer Security Assoc

⚡ Kirk Enterprises: What's in a name?

Andrew Koenig <ark@research.att.com>

Mon, 5 Aug 1996 13:45:43 +0400

There is a small company in Indiana, called Kirk Enterprises, that makes various kinds of gadgets for attaching cameras and lenses to tripods. I was interested in information about one of their products, so I thought I'd see if they had a web page.

I went to Lycos and did a search for `Kirk Enterprises.' What came back was a flood of references to Star Trek.

Andrew Koenig ark@research.att.com

[For oldtimers, that would rate well on the Kirkman Laugh Meter. PGN]

⚡ The increasing complexity of everyday life

<Rshek@aol.com>

Tue, 6 Aug 1996 09:47:52 -0400

One of my colleagues circulates Risks Digest here and I like to look through it. I was interested to read about the ever increasing complexity of life and the proliferation of remote controls, manuals, batteries, and the like. The risk here is not that the world will become overly complex and then fail, leaving us lost, blind, and bewildered. The risk, rather, is that we people will become overly dependent on external things and lose sight that what we require is inside us.

BUT what if the electricity and telephones go kablooie at the SAME time?? We can try any of the time honored activities of all human beings: we can tell stories, we can sing, we can dance, we can think, we can meditate, we can talk to the people who share our houses or apartments or dorms, we can light candles, we can build fires, and we can read books. With so many new tools and technologies it is easy to think that without the latest or our favorite we can't thrive or succeed or have fun or be ambitious. But that is fallacy. The best use of technology is to blend it with our human powers.

Department of Motor Vehicle records available On-Line

"Rich Ellermeier" <richarde@pcx.ncd.com>
Wed, 7 Aug 1996 13:20:45 -0700

In the State of Oregon, it is legal to purchase Department of Motor Vehicle Records from the state (RISK 1). These records have been

purchased, placed
on a CD and made available through a newspaper advertisement.
Now, on a
local ISP, someone has made these records available publicly via
a data
base search based on the license plate (RISK 2). After looking
at the data
with some friends, we have found that some of the information
is, in fact,
wrong or out-of-date (RISK 3).

RISK 1: The state of Oregon should NOT be allowed to make
available this
information. Among the type of information that will be
displayed:

- vehicle type, make, model, year and style
- vehicle Identification Number (VIN)
- vehicle title number
- Plate expiration date
- Owner name, address and Driver's License number (For ALL
owners)
- Security interest holder and their address.

RISK 2: The ease of access may cause this information to be used
in a illegal
manner. By hanging out at the long-term parking lot of an
airport,
one would be able to identify the name and address a
traveler making
that traveler's home vulnerable to thieves. This
information could
easily be used by stalkers and those who wish to have
their privacy
protected. An unlisted phone number and address in the
phone book
is easily circumvented when that information is easily
accessible
with just a license plate number.

Risk 3: A friend sold a car five months ago, yet in this
database, he is
still identified as the owner. Should the new owner do
something

on the road that provokes "road rage" in another driver, a quick search of the data via license plate number will find that my friend is the owner and the potential for him becoming a "road rage" victim increases, through no fault of his own.

It strikes me that there are multiple parts of the problem that need to be fixed. The DMV should, by law, not be able to sell this information. However, the one issue that I believe the internet/web has not come to terms with yet is the one that has always plagued a free society--the limits of that freedom. While it may be legal to make this information available in this manner, the moral and ethical implications of doing so need to be carefully considered.

--rich <richarde@pcx.ncd.com>

⚡ "Anonymous" phone tips and Calling Number Identification

Michael Cook <mlc@iberia.cca.rockwell.com>

Thu, 8 Aug 1996 09:26:44 -0500

I thought I'd pass along something that has recently happened at my company.

This summer, we had a new phone system installed, with fancy phone features of various kinds, voice-mail for each phone, callback, conference calls, etc.

One of the features is Calling-Number Identification. When a call is received, the incoming phone number is display on our phones.

If the call is from a company extension, that person's name (or some group function name) is also displayed. (So, the usual Caller-ID good/bad points are raised.)

For some time, our company has had an anonymous Ombudsman phone number for reporting suspected company ethics violations or other business policy misconduct. But with the new phone system, the Ombudsman phone had CNID! Not-so-anonymous reporting.

To its credit, the company has installed a new phone line.

"Since the installation of the new ... telephone system, concern has been expressed that employees can no longer make an anonymous report of a violation or suspected violation. A new phone line has been installed that cannot display phone numbers of incoming calls. Those wishing to remain anonymous may call ..."

I haven't checked yet whether it is possible on our system to block CNID on selected phone calls.

Michael Cook MLCOOK@CCA.ROCKWELL.COM

✉ Re: Where Wizards Stay Up Late ([RISKS-18.29](#))

Danny Cohen <cohen@rand.org>
Thu, 01 Aug 96 14:30:45 PDT

.. and why the service was so bad across the country, why both

dropped 40%?

> Perhaps the real problem is that the wizards are no longer staying up late
> enough, or that the new quasiwizards are not familiar enough with history
> and the sense of accomplishment that prevailed in the ARPAnet days. [PGN]

The reason is not lack of sense of history. My first computer/computer communication project was done in summer 1967 for Larry as he moved from LL to ARPA. I can relate to your concern about that "lack of sense of history").

The reason is that now someone must pay for the packets to travel. It was nice in the old days when Larry and Bob willingly paid for all our packets. Now they don't. No wonder that the existing charging mechanism pushes the demand beyond the supply. Larry, Bob, Vint, and others (in ARPA, NSF, DoE, and NASA) took it upon themselves to always provide excess supply (at least they tried to).

Most users believe that they have a constitutional right for free network services since most scholars would agree that packet communication falls under "the pursuit of happiness". The present charging scheme encourages exponential growth of the demand, limited only by the frustration caused by the insufficient supply. If you were willing to pay the real cost of that Telnetting, the packet would have gone through. This is what many corporations do. Phone calls go through because we (or someone else) pay

for each. We, who are used to practically free rides suffer.

If you really want to help solve the problem you better introduce the subject of "RISKS of not paying for what you get". Sigh.

It used to be so nice when they paid for us... Danny

⚡ Re: IBM's Olympic Systems

Dave Wortman <dw@pdp1.sys.toronto.edu>

Fri, 2 Aug 1996 10:27:44 -0400

Since there's been a lot of discussion of the IBM Computer Systems deployed at the Atlanta Olympic games, some might be interested in IBM's description of the system at:

http://www.olympic.ibm.com/o_tech/index.html

The link

"Everything else you'd like to know about IBM's 1996 Olympic Games Activity"

leads to fairly comprehensive documentation.

[Incidentally, I am happy to hear from various sources reports that things

have settled down since the early problems of these Olympic Games. PGN]

⚡ re: Computers causing power outages (Sessions, [RISKS-18.29](#))

Paul Peters <PPeters@DOCKMASTER.NCSC.MIL>

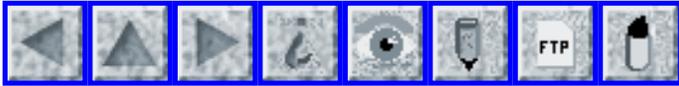
Fri, 2 Aug 96 12:37 EDT

In the subject posting, D.C. Sessions states that "Constant-power loads exhibit negative resistance". While they present a non-linear load, there is no reasonable way to describe them as negative resistance. He further confounds his thesis by using the electric light as an example of constant impedance. The incandescent lamp is a highly non-linear impedance and more closely resembles a constant-power load than it does a constant impedance load.

Paul E. Peters



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 18: Issue 31

Friday 9 August 1996

Contents

- ["Buffer overload" crashes network bridge](#)
[Jeff Anderson-Lee](#)
 - [Re: America Offline](#)
[David Kennedy](#)
[David Cassel](#)
 - [Re: AOL outage: risks of scaling inappropriately](#)
[Jeff Hayward](#)
 - [Re: Kirk Enterprises: What's in a name?](#)
[Jeffrey Mogul](#)
 - [Novel: Slow River](#)
[Steve Kilbane](#)
 - [Re: The increasing complexity of everyday life](#)
[Barry L. Brumitt](#)
 - [Re: Department of Motor Vehicle records](#)
[Lauren Weinstein](#)
[Steven Bellovin](#)
[C. Titus Brown](#)
[A.E. Siegman](#)
[Kevin Johnsrude](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ "Buffer overload" crashes network bridge

Jeff Anderson-Lee <jonah@shiva.CS.Berkeley.EDU>

9 Aug 96 17:16:35 GMT

End of summer... time for the floors to be buffed before the students come back. So the custodians bring out their heavy duty floor buffers and plug 'em in. Given the old, out-of-date wiring in this building they blow a circuit. Instead of resetting the breaker however they just try another outlet and keep going. The result: the network bridge on that circuit is put out and half the net is cut off from the other half.

Of course we had trained the custodian NOT to do this in the past, but that particular custodian is off on sick-leave, and their replacement had not been so briefed. Fortunately someone remembered the previous time this happened and found the problem. But what happens if they go away too?

Jeffrey Anderson-Lee

[You shuffle off to buffer-low,
without getting too big for your bridges. PGN]

⚡ Re: America Offline ([RISKS-18.30](#))

David Kennedy <76702.3557@CompuServe.COM>

09 Aug 96 12:56:47 EDT

Courtesy of the Dow Jones News Service via CompuServe's Executive News Service:

AOL's Blackout Eclipses Jump In Fourth-Quarter Profit
By Thomas E. Weber and Jared Sandberg, Staff Reporters of
The Wall Street Journal (Dow Jones, 9 August 1996)

>> It wasn't until late yesterday that AOL provided a detailed
>>explanation for the outage to supplement Chairman Stephen M.
>>Case's on-line apology, which AOL posted late Wednesday night.
>>The company cited a "coincidental" series of events it said are
>>unlikely to recur. The problem centered on routers,
>>computerized switches that serve as traffic cops for
>>information on AOL's complex network.

>> Computers at an AOL unit fed these switches with an erroneous
>>"roadmap" of the Internet just as engineers were upgrading
>>them. When problems cropped up, the engineers mistakenly
>>thought their upgrade was to blame -- not the roadmap. That
>>misunderstanding delayed discovery of the source of the
>>problem. Compounding the confusion, diagnostic software that
>>could have helped track down the problem had been turned off
>>during the upgrade, AOL said.

o AOL is compensating customers with one free day's worth of
connect time.

[DMK: I pay US\$9.95/mo for AOL and get 300 min-->10min/day or US\$0.33/
day.

Give me a break!]

o In a letter to subscribers, Mr. Case said:

>>I would like to be able to tell you that this sort of thing
>>will never happen again, but frankly, I can't make that
>>commitment, as we are building a new medium and breaking new ground.

and

>>This was a very unfortunate occurrence and I don't want to make
>>light of that. But it did have an interesting side effect: it
>>reminded all of us how important AOL is becoming in our
>>everyday lives.

and closes with

>>Today's outage reminds us that despite the recent progress
>>we've made in expanding our AOLnet network and enhancing the
>>responsiveness of our Member Services team, we still have a
>>long way to go to make AOL as reliable as must-have utilities
>>such as electricity and the telephone. But that's what we
>>intend to do.

Dave Kennedy [CISSP] InfoSec Recon Team Chief, National Computer Security Assoc

[MODERATOR'S CORRIGENDUM: Typo (should have been 6 million subscribers) in [RISKS-18.30](#) fixed in archive copy. Oddly, no one remarked on it, but I stumbled onto it myself! PGN]

🔥 Re: America Offline ([RISKS-18.30](#))

David Cassel <destiny@crl.com>
8 Aug 1996 15:27:28 -0700

AOL issued a statement early Wednesday saying service would be restored Wednesday afternoon. In fact, it didn't go up until 11 pm.

Subscribers trying to log on received the following series of messages.

"The system is temporarily unavailable. Please try again in 15 minutes."

"The system is temporarily unavailable. Please try again in 30 minutes."

"The system is temporarily unavailable. Please try again in an hour."

"The system is temporarily unavailable. Please try again in 90 minutes."

This kind of thing is going to get AOL a reputation for dishonesty. The Wall Street Journal wrote, "AOL put out a puzzling press release claiming that [newly-hired Chief Operating Officer] Razzouk had chosen to resign largely because he didn't like 'the prospect of relocating his family to the Washington, D.C. area.' Never mind," the Journal added, "that Mr. Razzouk

had, in truth, just sold his Memphis home -- and that he had already closed on the purchase of a new \$1.7 million showplace in McLean, Va."

But technical misstatements will always come back to haunt you.

Earlier

this week an AOL rep told the *San Francisco Chronicle* that AOL's computers

were "immune" to the kind of outage that occurred yesterday. And days after

AOL told a content provider they'd fixed a security hole, hackers used it to

take the stage during an on-line celebrity appearance, taunting the regular

guest...

The day after they came back on-line, their system was automatically displaying the worst possible messages. The mandatory-viewing ad pitching

more time on the system began, "We know that many of you have been reluctant

to fully explore the diverse offerings..." The "Top News Story" in their

Reuters headline area turned out to be "AOL Apologizes for Massive Outage."

And the sign-off ad: "This week: 'Gravity Kills' ".

"We can't definitively state the root of the problem," AOL's Vice President

told Reuters that night. The ultimate irony: just last month AOL took out

help-wanted classified ads saying "At America Online, we not only dominate

the programs we design...."

David Cassel

<http://www.crl.com/~destiny/time.htm>

[David, "dishonesty" sounds a little harsh. How well can anyone predict how long it is going to take to fix a problem that has not yet been identified and understood? PGN]

🔥 **Re: AOL outage: risks of scaling inappropriately (Snyder, [RISKS-](#)**

18.30)

Jeff Hayward <J.Hayward@utexas.edu>

Fri, 9 Aug 96 12:08:29 CDT

Joel Snyder writes of the widespread effects of the AOL outage on mail systems throughout the Internet.

While I agree that there are some interesting risks in putting so many user's eggs in the "@aol.com" mail basket, the severe consequences of an AOL outage on (other) mail systems can be looked at as different sort of inappropriate scaling risk - the inability of the majority of mail systems in the net today to handle the large queues and outages that are the reality of today's Internet.

The vast majority of mail systems in the Internet rely in one way or another on mail transfer software that was never designed to scale well - often the much maligned but mostly essential "sendmail" program. Among sendmail's well know faults are its handling of the backlog queue as a single batch, and its lack of ability to schedule retries for unreachable hosts on any but the most simple-minded basis. In the event of an outage creating a large queue this can effectively deliveries for everyone as the system tries and tries to deliver undeliverable messages.

Fortunately for me, for the week prior to the AOL outage I had been running the outbound mail from one of my mail servers through a system running qmail, a mail transport system designed as ground-up replacement for sendmail. (See <http://pobox.com/~djb/qmail.html> for more information). The two features of qmail that kept the mail flowing for me during the AOL outage are (1) delivery attempts are scheduled independently for each message in the queue, and (2) delivery attempts are scheduled following a backoff algorithm that prevents the retries from consuming the mail

system

as the backlog grows. So for my site, the AOL outage was a non-event. The backlog for AOL grew and grew but mail for other sites continued to flow expeditiously and load on the server was nearly constant. When AOL became available again, there were no major load spikes delivering the backlog because the delivery retries were well spread out in time. I had to do nothing extra to keep things going - a new experience for me!

So I don't see the risk(s) as necessarily one-sided. AOL has some whale-sized scaling problems to overcome to be sure, but sites that depend on simple-minded mail delivery software should consider their own exposure, and investigate software designed with modern conditions in mind if they want to keep delivering the mail. -- Jeff Hayward

✦ Re: Kirk Enterprises: What's in a name? (Koenig, [RISKS-18.30](#))

Jeffrey Mogul <mogul@pa.dec.com>

Thu, 08 Aug 96 17:50:23 MDT

Andy writes:

I went to Lycos and did a search for `Kirk Enterprises.' What came back was a flood of references to Star Trek.

Of course, the real "risk" here was that of using the wrong search engine.

I tried "Kirk Enterprises" (the "'s are significant) in AltaVista, and got exactly 20 responses, not one of which contained the work "trek".

-Jeff

🔥 Novel: Slow River

<Steve_Kilbane@cegelecproj.co.uk>

Fri, 9 Aug 1996 14:16:53 +0100

RISKS readers with a fondness for near-future sci-fi might like to check out Nicola Griffith's novel "Slow River". Much of the plot is concerned with the safe operation of a water purification plant, in the face of bad management and staffing problems.

steve

🔥 Re: The increasing complexity of everyday life (Shekerjian, [RISKS-18.30](#))

"Barry L. Brumitt" <belboz@FRC2.FRC.RI.CMU.EDU>

Fri, 9 Aug 96 11:56:40 EDT

Rshek@aol.com asks "What if the electricity and telephones go kablooie at the SAME time??", and posits that there are a myriad of activities which human beings can engage in which are independent of these pursuits. However, it remind me strongly of an episode of "Connections" by James Burke which I believe was entitled "Technology Trap." In light of the famous power east coast power outage in the late 60's, he examines carefully what might really happen if such a disaster occurred.

Comp.risks is for a discussion of the risks from computers and technology. I'd encourage anyone who is interested in this field who has **not** seen this episode to seek it out and view it. It's scary, enlightening, and perhaps the

best presentation of how Risky our dependence on technology can be...

Barry Brumitt Robotics Institute, Carnegie Mellon University

ps. It was originally a BBC program. Videotapes are available. Check your

local library.

✈ Re: Department of Motor Vehicle records (Ellermeier, [RISKS-18.30](#))

Lauren Weinstein <lauren@vortex.com>

Fri, 9 Aug 96 00:28 PDT

On the matter of Oregon DMV records being made available on the net, news

reports have indicated (I have not checked this personally) that the private

party who put them online has removed them, apparently after a very negative

reaction.

However, this of course does not prevent others from doing so, and the information already out there on those CD-ROMs can never be recalled

(though the accuracy will of course fade over time).

Of more importance in the long run is the incredibly bad policy of making

that data easily available at all. Now that use of SSNs for DMV records has

been mandated nationally, easy access to DMV information poses even more of a risk.

Down here in California, access to DMV records is now severely limited,

prodded mainly by a number of celebrity stalking cases where DMV records

were involved. Oregonians might consider looking to California for leadership on this topic.

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

⚡ Re: Department of Motor Vehicle records (Ellermeier, [RISKS-18.30](#))

Steven Bellovin <smb@research.att.com>

Fri, 09 Aug 1996 07:27:21 -0400

There has recently been a great deal of outrage about someone putting the Oregon license plate database on the Internet. That's not the problem -- the real problem is that the data is available at all. Many states make such data available, and there have long been people with complete files of such things. The only thing different here is that it was more easily available to the general public, with a fee.

In fact, more comprehensive services are already on the Web. It took about 10 minutes with AltaVista to find several similar services, though in some cases it wasn't clear if they actually did business over the Net, or simply used it for advertising.

The Web has become a microcosm of our society. If it's out there, it's on the Web -- and if it suddenly shows up on the Web, it's probably because it was already out there, but you didn't know it.

--Steve Bellovin

⚡ Re: Department of Motor Vehicle records (Ellermeier, [RISKS-18.30](#))

C. Titus Brown <brown@reed.edu>

Thu, 8 Aug 96 22:19 PDT

While it may be a valid point that the Internet/WWW has not come to terms with the limits of the freedom, I don't believe that issue can be linked with the issue of the DMV making records available.

Simply, the DMV should not have made this information available. Whether or not "the Internet" should have taken this information and distributed it in such a manner is besides the point.

It is virtually inevitable that all information not strictly kept under wraps will make it onto the WWW. Blaming the WWW (or the Internet) for this is senseless.

ObRisk: This sort of thought process (blaming the accessibility of information on the medium used to transport, not the provider) is what leads to things like the CDA: censorship too late & targetted on the wrong thing.

--Titus

✉ **Re: Department of Motor Vehicle records (Ellermeier, [RISKS-18.30](#))**

AES <siegman@ee.stanford.edu>

Thu, 08 Aug 1996 17:29:39 -0700

Let me disagree:

- 1) There are important reasons (law enforcement, traffic accidents) for making this information rapidly available to police officers down to very low (small community) levels. Once you do this, the information is so easily compromised (I can overhear this kind of information on a police scanner any evening) that it's better that it be just plain public, and let everyone know that it is.
- 2) If RISKS 2 and 3 above are the best that can be cited for not making such information available, they seem to me pretty

negligible.

When my car is at the airport, several other people and two large dogs are likely still at home -- if this thief drives the 30 minutes

to my house, he'll pretty disappointed. "Road rage", especially in combination with CD-ROM ownership, I suspect is statistically insignificant, if not mostly an urban legend.

3) There are certainly other legitimate reasons for making this data available. If some clever inventor comes up with an add-on that will lower the pollution and raise the mileage (currently 12 mpg) of my beloved classic '67 Mustang, for example, I'd love to have him scan the DMV database and send me a sales message. One can think of many other health and safety as well commercial reasons for being able to find the owner of a car rapidly.

🔥 Re: Department of Motor Vehicle records (Ellermeier, [RISKS-18.30](#))

"Kevin Johnsrude" <kevinj@roguewave.com>

Fri, 9 Aug 1996 10:23:04 PST-8

With regard to informational privacy and the state of Oregon's selling of DMV data, the Cyberspace-Law list indirectly makes a number of interesting points:

Consider 4 cases:

(1) Your local supermarket offers a "No-coupon discount card" for customers who fill out an application. On the application, you list your name, your sex, your income, your employment, and the company gives you a card. Using the card, you then make purchases for the next year. The supermarket then compiles the data about your purchases, and sells it to marketers. You have not been notified that they intend to use the information like this; nor have you explicitly consented to this use.

(2) Your credit card company has the same information about you -- you supplied it when you got your credit card. Imagine it now collects the data

about your purchases, and then sells it to marketers.

(3) Your local video store keeps data about the videos you rent. It then sells to marketers your name and address, along with list of films that you have rented.

(4) A credit card company enters into an agreement with the IRS, to report to the IRS people whose spending habits change dramatically. The IRS then uses that data to help it decide which returns will be subject to audit.

All four cases raise the problem of *informational privacy* -- the question how much control, if any, does the law give you over the collection, and dissemination, of information about you that you have willingly given over to someone else. The answer in general is quite simple: Not much. American law in the main gives individuals very little control over what others can do with the information collected about them.

This lack of protection distinguishes American law from most European democracies. "Data protection" is an important part of European human rights law. But with slight exceptions, it is not an important part of our tradition. The exception is case (3): Because of the outrage over the publication of Judge Robert Bork's video rentals when he was nominated for a seat on the Supreme Court, Congress passed the Video Privacy Protection Act of 1988, which makes it a crime to release individualized data about the videos any individual may rent or buy.

At least that part of your "record" is protected: but not what books you check out at the library, or what your purchases at the grocery store are, or what movies you use your credit card to buy tickets for. These

remain unregulated by the law.

Consider 4 more cases:

(1) On a local university network, users can read USENET news stories -- stories posted on the USENET bulletin boards by users from across the world. The stories range from discussions of technical material about computer operating systems, to highly controversial political discussions, or to discussions about sexuality. Imagine now that network users can use a simple command to list all other users logged onto the system at that time, as well as what those users are doing. If the users are reading news stories from the USENET new server, then the command will report to the users what news stories they are reading.

(2) An activist group is angry about pornography on the net. It decides to attack the problem in a somewhat unique way. It opens up an erotic web site, and then as individuals access the web site, the group collects the information about who accessed the site. On a separate web site the group then publishes a list: "Known consumers of pornography" and then lists the information it has about people who have accessed its site. Or imagine the same case, with slightly different facts: Imagine the activist group is an anti-gay activist group, and it puts up a web site on resources for gay and lesbians, and then publishes the lists of who accesses the site. Or an anti-abortion group, that publishes information about access to abortion clinics.

(3) Some World Wide Web browsers collect a list of the web sites that you have accessed. This list is kept on your machine. When you

access a web site, the software makes it possible for the web site to read the list of web sites that you have previously accessed. Imagine that a web site has implemented a procedure to read your list of web sites, and then decides whether to admit you based on what other places you've been. (In a sense, the system is discriminating in granting access, but what is important for our purposes is that it is making that discrimination by accessing "your" information about where you have been.) For example, if it determines that you don't frequent sufficiently "posh" places, it bumps you; or if it surmises from your list that you are a Republican, it bumps you.

(4) As we explained in case (1), USENET is a cooperative that distributes messages in the form of discussion threads, on wide range of topics, to millions of people across the world. People can participate in these discussions, simply by replying to a particular message. This reply then gets published across the world, with the email address of the person replying to the message attached to the reply. Ordinarily, these messages disappear after a few weeks on the net. [Not RISKS and many others... PGN] But imagine a company starts collecting these messages, and begins organizing them in a data bank. This company then makes it possible for anyone, through the Web, to search the database of USENET messages, for a particular word, or phrase, or for the name of a particular user. This search then collects all messages that have that word, or phrase, or name, and displays the list of messages, along with their senders. The user of this service can then click on the name of the senders, and get a profile of all the messages that person has sent. For example the user can discover

that the sender of a particular messages has regularly contributed to a discussion of leftist politics, or a pro-life discussion group, and then access all of the messages this sender has sent to these groups.

All four of these cases raise no legal problem at all, given the present state of United States law. Examples (1), (3) and (4) already exist. (Netscape would support a function like example (3); for example (4), check out <http://www.dejanews.com>); we don't know of an example of case (2), but there is nothing in the law to stop it. Again, as we indicated in our last message, the law does very little to protect individuals against the use of data that they make available to others. Each of these 4 cases is just an example of this same point.

It is not hard to understand why the law has been so unprotective. For the most part, historically, it has been relatively difficult to get access to data like this. Perhaps one could hire a spy to follow an individual around and collect information about his habits, or purchases -- no doubt some people did. But for the most part, people didn't pay much attention, since it was very costly to pay attention. The dramatic change in data technology has changed this. Now it is quite easy to collect a vast amount of data about individuals. More importantly, now it is quite profitable to collect such data. Cyberspace will only make this more so. We are living in a time when the law has not caught up with the technology. While the inefficiency of technology provided some sort of protection before, now nothing -- neither law nor inefficiency -- protects us today.

Do we want protection? Not clear. There are interests that pull the other way: Some have argued that there is a first amendment right to

report

to others true facts they have found out about you. Others have argued that

this information would be a real gain to the efficiency of the market: Imagine, for example, advertising that was perfectly targeted to those, and

only those, who would be likely to buy a particular product.

Cyberspace law WWW page:

<http://www.counsel.com/cyberspace>

To SUBSCRIBE to Cyberspace-Law, send a message to

LISTPROC-REQUEST@COUNSEL.COM

with the command

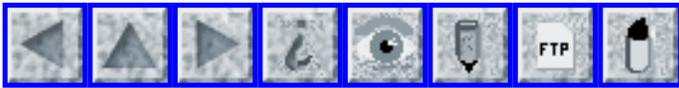
SUBSCRIBE CYBERSPACE-LAW Firstname Lastname
in the body of your e-mail, (replacing "Firstname" and
"Lastname" with your first and last names -- or such
pseudonyms as you prefer).

**** Back to Kevin Johnsrude: Clearly the OR DMV is not doing anything illegal under the law. Your phone company does the same thing: when you pay your US\$0.25/month not to get telephone solicitations, you are, among other things, recompensing your phone for not *selling on a list* your name, phone number and address to telemarketers. Your VISA company also does the same thing and gives marketers your complete personal and financial profile.

We in the US desperately need better data privacy protection or we will effectively not have any privacy at all.

--KevinJ

Kevin Johnsrude, Software Design Developer, Rogue Wave Software, 850 SW 35th St., Corvallis, OR 97333 Email: kevinj@roguewave.com Voice: (541) 754-3010



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 18: Issue 32

Tuesday 13 August 1996

Contents

- [Java security update](#)
[Ed Felten](#)
- [More power to us? "It couldn't possibly happen again" department](#)
[PGN](#)
- [Another London train crash; well, it's not supposed to happen!](#)
[PGN](#)
- [Fire alarms on Boeing 777 triggered by fruit/frog cargo](#)
[PGN](#)
- [Electromagnetic pulses to stop car chases?](#)
[Peter Wayner](#)
- [GPS Receiver Explodes](#)
[David Kennedy](#)
- [Bread-riots and circuses](#)
[Brian O'Connell](#)
- [The risks of apathy in telephone callers](#)
[Christopher Kline](#)
- [CyberRisk '96 Conference, Call for Participation](#)
[Mich Kabay](#)
- [Re: Computers causing power outages](#)
[Paul Hughett](#)

- [Re: "Anonymous" phone tips and CNID](#)
[Jeffrey Mattox](#)
 - [Re: Department of Motor Vehicle records](#)
[Steve Sapovits](#)
[Benedikt Stockebrand](#)
 - [Re: America Offline](#)
[James K. Huggins](#)
[Matthias Urlich](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ **Java security update**

Ed Felten <felten@CS.Princeton.EDU>

Mon, 12 Aug 1996 20:29:06 -0400

We have found two Java security bugs recently, one in Microsoft Internet Explorer 3.0beta3 and one in Netscape Navigator 3.0beta5. Both bugs were serious, allowing a malicious applet to gain at least full read/write access to the victim's files. Both bugs are fixed in current releases of the browsers.

The Netscape bug was caused by incorrect handling of type definitions in the Java internals. Java uses special predefined names for its array types; these special names are bound to the correct array types on demand. We discovered that under certain circumstances an applet could define a class that had one of these special names. The system detected this and threw an exception, but the malicious definition was mistakenly left in one of the system's internal tables. The result was that an applet could redefine one

of Java's array types. This was sufficient to break Java's type system and hence to circumvent Java's security mechanisms.

The Microsoft bug allowed an applet to become a member of a security-critical Java package (module) whose membership was supposed to be limited to Java classes that are built-in to the browser. Code belonging to one of these packages can set certain security-critical variables such as the access control lists that say which files the applet is allowed to read and write. An applet could exploit this bug to obtain full file system and network access, among other things.

For more details, see <http://www.cs.princeton.edu/sip/News.html> or contact Ed Felten (felten@cs.princeton.edu, 609-258-5906).

Dirk Balfanz, Drew Dean, and Ed Felten, Safe Internet Programming Group,
Department of Computer Science, Princeton University

[The "current release" of the Microsoft Internet Explorer is the one that was available at midnight PDT at the end of Monday evening (i.e., 3AM EDT Tuesday 13 Aug). RISKS suggests that serious users of either browser pick up the new versions, and that people who consider themselves only casual users get more serious. PGN]

⚡ More power to us? "It couldn't possibly happen again" department

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

Tue, 13 Aug 96 00:12:19 PDT

Power losses on 10 Aug 1996 (Saturday) affected at least 4 million customers in 8 U.S. states from Canada to Mexico (including parts of Texas). San Francisco Airport was reduced to a mass of waiting humanity in the absence of power other than air-traffic-control emergency power that permitted just a few planes to take off. Many landings were diverted and many flights cancelled.

Outages were spotty. For example, Palo Alto was down for 5 hours, while neighboring Menlo Park seems to have been (mostly?) unscathed. (Perhaps SRI's cogeneration plant helped out!) Some places were still out the next day.

The Pacific Intertie between Oregon and California was reportedly involved again, but according to a late report (CBS late TV news) only as the 26th in a series of thus-far-identified problems that began with three line outages (hot weather expanding power lines), a problem at the Washington-Idaho boundary, and another problem at the McNary substation. The CBS report suggested chaos theory as an explanation, with many small causes combining in unexpected ways to cause something that allegedly is not supposed to happen. Unusually hot weather in Washington and Oregon and heavy use of air conditioners everywhere in the West contributed significantly. (I suppose Saturdays require much less commercial AC, but much more home AC.) An earlier theory that this new problem had been caused by a fire

under some transmission lines seems to have fallen by the wayside -- the fire apparently occurred after the outage had been triggered. Of course, the computer controlled systems did exactly what they were supposed to do -- shut down when threatened with overload conditions that might be damaging to the system.

The early July 1996 outages had very similar but less long-lasting effects.

(The 2 July outages spanning 12 Western states were apparently triggered by a single tree in Idaho, as noted in [RISKS-18.27](#), but also occurred during a hot spell.) It appears this might become a commonplace occurrence. Some power officials said that this was a really freak (i.e., very unlikely) occurrence, while others perhaps more candidly said there is very little they can do to prevent further recurrences.

An emergency meeting of utilities folks is taking place this week, to consider what might be done differently. I suppose they might recommend we all wear lighter clothing and offer frequent-flier miles for recycled perspiration. But serious suggestions might include cutting down more trees? Shutting down more salmon ladders? Perhaps instituting more rolling brownouts? How about more preventive maintenance? More oversight? Closer local monitoring and more integrated/distributed system-wide monitoring? In the 11 Aug case, diagnostics apparently indicated that a massive problem was imminent something like half an hour beforehand, but those warnings were

evidently not given sufficient priority.

And then Monday afternoon, 13 August, there were new outages. South San Jose -- which was partly spared on 11 August, including a Neil Diamond concert -- was hit this time with some long outages; the Hicks substation apparently had a transformer explosion, affecting 27,000 customers. Palo Alto (which has its own utility company, but depends on PG&E) had a 45-minute outage that affected all 29,000 customers; the outage was blamed on PG&E having messed up by sending an erroneous control signal to Palo Alto.

Please pardon any inaccuracies here. There still seem to be a lot of unknowns, and the reporting is itself spotty. I hope when all the smoke clears, we get some definitive analyses for RISKS. This is clearly a very important topic for us to contemplate, because we are increasingly dependent on our power infrastructure for our computing/communication/transportation/... infrastructure, which increasingly depends on our power infrastructure, etc. Also, the long-term weather prospects (including global warming, if you care to believe in it) and dramatically increased usage demands seem to suggest more problems in the future.

⚡ Another London train crash; well, it's not supposed to happen!

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

Mon, 12 Aug 96 10:09:48 PDT

A London commuter train carrying about 400 passengers from Euston Station crashed into an empty train heading into Euston Station, killing one passenger and injuring about 100 near Watford Junction in Hertfordshire, 20 miles north of London, in the afternoon rush-hour on 8 Aug 1996. [Source: *San Francisco Chronicle*, 9 Aug 1996, A12]

No cause was given, but of course the signalling system is supposed to prevent that from happening. (The RISKS archives include a bunch of incidents on trains in and around London.)

🔥 Fire alarms on Boeing 777 triggered by fruit/frog cargo

"Peter G. Neumann" <neumann@csl.sri.com>
Sun, 11 Aug 96 10:44:12 PDT

False alarms on the Boeing 777 are apparently being triggered by unusual humidity and temperature conditions in cargo holds. For example, a London-bound Emirates aircraft was diverted to Cyprus, due to heavy-breathing mangos, and a Cathay aircraft was evacuated and the fire-suppression system activated -- due to a combination of fruit and frogs. Apparently, tropical fruit (and especially durian fruit) generates enough humidity to be detected as smoke -- thereby triggering the alarms.
[Source: *Aviation Daily*, 12 Aug 1996]

[I wonder what this could do to a computer system, such as a spilled-pitcher-of-durian Cray? Also,

smoking mangos can be hazardous to your health? PGN]

✦ Electromagnetic pulses to stop car chases?

Peter Wayner <pcw@access.digex.net>

Sat, 10 Aug 1996 19:55:29 -0400

Police prepare stunning end for high-speed car chases
BY GILES WHITTELL AND NIGEL HAWKES, The Times, London, 10
Aug 1996

It could be the end of the car chase as we know it. With the automotive equivalent of a stun gun, science fiction is coming to the aid of law enforcement. A high-powered electrical device under development at the Pentagon's Army Research Laboratory in Adelphi, Maryland, is to be tested by police and border patrol agents and could be in use by next year.

The car stopper works by focusing an intense electromagnetic charge on the electronic systems that manage most modern engines, disabling them and paralysing the car. In the jargon of its inventors, the 150 kilovolt charge is a nemp, or non-nuclear electromagnetic pulse. Contractors are bidding to produce a police version.

Very precisely directed beams are required, but even then there will be problems. A pulse powerful enough to disable an engine at any reasonable range would also be likely to disrupt communications, damage television and radio sets, disable computers and even stop heart pacemakers. There is also the danger of loss of control when a car is being driven at high

speed.

Counter-measures would include using old-fashioned engines with no electronics, or perhaps surrounding the most delicate components with shielding. The best might be to get hold of one of the stun guns and use it to disable pursuing police vehicles.

✈ GPS Receiver Explodes

David Kennedy <76702.3557@CompuServe.COM>

09 Aug 96 17:28:42 EDT

Excerpted from the c4i-pro mailing list. A PLGR is milspeak for a Precision Lightweight GPS Receiver made by Rockwell. Note there are no conclusions in the report IRT whether the equipment was at fault or something else.

>Date: Thu, 08 Aug 96 16:18:00 +6

>From: Potter B MSgt ACC/SCXX <potterb@ns.langlely.af.mil>

>Subject: c4i-pro PLGR Violent Venting at Ft Irwin, CA

>

>Potter B MSgt ACC/SCXX <potterb@ns.langlely.af.mil>

>

>Urgent traffic regarding explosion of PLGR. Please forward to PLGR users at

>your units.

>

> Very Respectfully,

> //Bob//

> ROBERT A. POTTER JR., MSgt, USAF

> Readiness Branch

>

> -----

>From: Gray, Rodney, Lt CZU[SMTP:GrayR@gps1.laafb.af.mil]

>Sent: Wednesday, August 07, 1996 10:59 AM
>Subject: PLGR Violent Venting at Ft Irwin, CA

>

>The following point paper describe[s] the PLGR venting issue.
Please

>disseminate this message to the necessary people with your
services.

>

>Issue:

>

>On 30 July 96 a PLGR explode[d] during operation at Fort Irwin,
CA.

>Apparently there was a violent venting vice a slow vent. In
other words the

>PLGR case did not contain the blast.

>

>Discussion:

>

>The incident involved the Commanding General of the 4th
Infantry Division,

>Major General Kern, and his driver. The driver was injured by
the blast.

>His left eye was bruised, he did however make a full recovery
and was

>released from the hospital.

[DMK: Incident is under investigation. Rockwell has been
notified. This is the
first reported incident of this kind. Over 55,000 units have
been in the field
in the military for some time now.] ...

>Recommendation:

>

>This is initial report. Don't have enough information to make
a firm

>recommendation at this time. Will send updates as the
situation unfolds.

>

> JPO's Interim Measure

>

>As an interim measure, until the investigation is completed the
JPO has

>recommended that all BA-5800 batteries be removed from
equipment when
>connected to vehicle power. HOWEVER, the removal of the BA-
5800 when being
>powered by another power source has operational
considerations. It
>typically will cause faster use of the memory battery
(estimated 3 months or
>less usage versus 1 year) causing the memory battery to fall
below the
>adequate power level. This results in the loss of COMSEC key.
Which in
>turn cause a lost of almanac and user waypoint data. USERS
SHOULD ASSESS
>THEIR OPERATIONAL IMPACT AND RISK BEFORE REMOVING THE BA-5800.
Further
>guidance will be provided pending the results of the incident
investigation.

Dave Kennedy CISSP InfoSec Recon Team Leader, National Computer
Security
Association

✶ Bread-riots and circuses

"Brian O'Connell" <oconnell@panix.com>

Sun, 11 Aug 96 22:18:02 EDT

Among the ramifications of the recently completed Olympics may
be an
under-noted economic risk, and implications for other sorts of
international
competition. Retailers in this country claimed (and I believe
some
statistics corroborated this claim) that because consumers were
engrossed in
the TV coverage of the games they were not out buying stuff at
their usual
rate. Retail sales were thereby depressed. If this is the case
some

speculation on the economic role of entertainment culture might be in order.

What would have happened, for example, if the Olympics were twice as long?
or if they were twice as interesting? Would the change in buying patterns have been doubly noticeable? Would economists have classified the blip as serious? What if TV was routinely so enthralling? Would the economy suffer? In short, what is the likelihood of a recession caused by an entertainment event? (If the risk is measurable a related risk would be to allow the Net to become too entertaining without first establishing a reliable e-payment system, so that collectively hypnotized consumers could still shop.)

Of course, the Olympics are a commercial event and as such are about creating demand for consumer goods as much as anything else. They need advertising dollars to make them run and therefore might safely be assumed to cause an economic lull and surge of proportional size. But when is demand-creation decoupled from actual consumption? How long can consumers be frozen in front of demand-creating spectacles without some of that effort going to waste? Other events aren't as predictable as the quadrennial games. Conventional wars, for example, don't depend on ad money and have proven to be a pretty good draw. Would a lengthy, televised one disrupt the domestic economy? Speaking of wars, what are the strategic implications of this sort of event-driven economic upheaval? If indeed the production of

information goods and consumption of other sorts of products
can become so
absurdly linked, would the DoD develop entertainment programming
designed to
economically paralyze a region? A swords-into-sitcoms approach
involving
the military redeployment of Bob Hope, who could so amuse the
golf-loving
citizens of another country that the resulting economic collapse
might bring
down a regime?

While Radios Marti, Moscow, and Free Europe, to say nothing of
the larger
phenomenon of American cultural imperialism have caused similar
effects for
years, I'm more interested in the perhaps-less-overtly-hostile
act of waging
economic inactivity. The theory, however, is the same -- if the
radio can
make us (or "them") want more democracy, or sneakers, it can
also make us
want to stay home and listen to the radio. Perhaps more
importantly, I
wonder if new technologies (the Net, again) might provide a real-
time way to
remotely instigate collective and real-life events.

All of this bread-and-circusing is to say two things, both of
which have
been said before. First, the creation of demand can be dicey; as
post-Pavlovian humans we're capable of -- and perhaps inclined
to --
salivating at the sound of the bell itself rather than the
prospect of food.
Second, information warfare probably means more than propaganda
and printer
viruses, and can likely be tuned to selectively affect all sorts
of
complicated and contingent networks, including an economy.

⚡ The risks of apathy in telephone callers

Christopher Kline <ckline@tc.cornell.edu>

Thu, 8 Aug 1996 13:35:57 -0400

Information Week (22 Jul 1996, page 12) reports that K&T Communications of Fort Worth, Texas has registered the phrases "I don't know", "I don't care", "Whoever", and "It doesn't matter" as names of long-distance carriers in Texas.

The risk? When you make an operator-assisted long-distance call from Texas and the operator asks which long distance carrier you would like to use, it is in your best interest to have a preference. K&T charges "approximately twice" that of the largest carriers.

Opening up the long-distance markets may help spur the growth of an information infrastructure, but whether or not it helps lower prices for consumers is an open question.

Christopher Kline Cornell University ckline@acm.org

[For folks who still have rotary dials, you may find an automated voice interface that lets you utter those phrases as well!
PGN]

⚡ Re: Computers causing power outages (Peters, [RISKS-18.30](#))

Paul Hughett <hughett@galton.psycha.upenn.edu>

9 Aug 1996 22:16:50 GMT

Paul Peters is technically correct but also misses a valid point. D. C. Sessions should have said "negative incremental resistance" rather than simply "negative resistance." The former term means that for some range of voltage, the current increases as the voltage decreases. This means that the power company cannot (necessarily) reduce the power consumption by reducing the line voltage, which has been the usual way of handling temporary power overloads without dropping service entirely; in fact, decreasing the voltage may now increase the power consumption, since line losses increase as you go toward lower voltage and higher current. What is perhaps worse is that a power supply, a negative incremental resistance device, and a few passive components can make an excellent oscillator; look up the circuit for a tunnel diode oscillator. In other words, the power distribution system becomes dynamically unstable, perhaps with rather large voltage and current excursions as all the passive and active components interact. Not something that I want to hook my house up to. By the way, "negative resistance" is frequently (if incorrectly) used as a synonym for "negative incremental resistance," and in fact this is the meaning that I assumed was meant in the original post.

Paul Hughtett University of Pennsylvania

✉ **Re: "Anonymous" phone tips and CNID (Cook, [RISKS-18.30](#))**

Jeffrey Mattox <jeff@cher.heurikon.com>

12 Aug 1996 17:46:31 GMT

Many people do not realize that most corporate phone systems have SMDR

(station message detail recording) which logs each call from each telephone.

So, even if CNID is disabled, it is very likely that a log exists of each phone call. It is a simple matter to search for calls to specific numbers.

Jeffrey Mattox -- jeff@heurikon.com

✶ Re: Department of Motor Vehicle records (Siegman, [RISKS-18.31](#))

Steve Sapovits <steves@telebase.com>

Mon, 12 Aug 1996 15:24:12 -0400 (EDT)

I'd argue that police access is different than public access. The police

have access to other forms of information the general public does not

have easy access to.

I don't buy arguments 2 and 3. If you personally want your information to be public for the sake of getting unsolicited advertising, then I have no problem with a system that allows you to give permission to do that.

The problem is where do you stop this? Using your first and last arguments, why not make all credit information public so that the police can easily detect credit card fraud and you can get targeted advertising

based on
your buying habits? Perhaps all educational and employment
records should
be made public so we can check resumes for accuracy. No
thanks. If people
want to make such information on themselves available, that's
fine with me,
but I want control over my own personal information.

Steve Sapovits N2K Telebase (<http://www.n2k.com>)
steves@telebase.com

✉ Re: Department of Motor Vehicle records (Ellermeier, [RISKS-18.30](#))

Benedikt Stockebrand <benedikt@devnull.ruhr.de>
12 Aug 1996 15:49:14 +0200

What's worse, some years ago the German RAF (Rote Armee Fraktion/
Red Army
Fraction), the major terrorist group of that time, allegedly (i.
e. it's too
long ago to remember my sources) used to somehow obtain access
to the
registration data of some vehicle, fake the vehicle registration
ID card
(Kraftfahrzeugschein), then steal a car of the same type and
color and fake
the license plates. Such a vehicle would pass any road block,
even if every
vehicle passing the block would be checked against a vehicle
registration
data base. Handing out the necessary data sure makes life
easier for some
folks.

Conclusions are left to the RISKS reader in general and the
security
and intelligence folks hopefully reading this in particular.

Benedikt Stockebrand, Dortmund, Germany

[Although RISKS truncates disclaimers, Benedikt added something to the effect that his name and e-mail address are not to be used in any way for advertising purposes, and that a fee would be imposed on unsolicited advertising (for proofreading costs). It remains to see whether any such disclaimers could be enforced, but perhaps RISKS should add one to the risks.info file! PGN]

✉ Re: America Offline (Cassel, [RISKS-18.31](#))

"James K. Huggins" <huggins@eecs.umich.edu>
Sun, 11 Aug 1996 08:47:21 -0400 (EDT)

[David, "dishonesty" sounds a little harsh. How well can anyone predict how long it is going to take to fix a problem that has not yet been identified and understood? PGN]

Exactly. In fact, this is one of the oldest problems in our field ... the fact that we don't know how to predict how long it will take to do just about anything useful (write new code, fix an old piece of code, etc.).

True honesty is all too rare in our discipline. How often will you hear a company say "We have a problem with our product. We don't know what's causing the problem, either. We're working furiously on it to solve it, but

we can't predict whether it will take minutes or days to fix it."? Consider also the common practice of marketing "bug fixes" as "upgrades" --- sometimes free, sometimes not.

⚡ Re: America Offline (Cassel, [RISKS-18.31](#))

Matthias Urlichs <smurf@noris.de>
11 Aug 1996 16:36:04 +0200

> [David, "dishonesty" sounds a little harsh. How well can anyone
> predict how long it is going to take to fix a problem that has not
> yet been identified and understood? PGN]

You can't, and that's the point. When I tell my customers "Try again in 15 minutes", they'll assume that I have enough data to make a reasonable guesstimate that the repair will take 15 minutes, more or less.

If, on the other hand, I haven't the faintest idea what's going on, then "we've had a major system crash, please try again later" would (a) be more honest and (b) would not annoy customers by raising unfulfillable expectations.

Matthias Urlichs noris network GmbH

⚡ CyberRisk '96 Conference, Call for Participation

Mich Kabay <75300.3232@CompuServe.COM>
12 Aug 96 21:20:22 EDT

CyberRisk '96

"Reducing risk and building ethical policies in the electronic workplace"

7-8 November 1996

National Airport Hilton, Arlington, Va.

Organized by the National Computer Security Association

FOR MORE INFORMATION:

WWW: <http://www.ncsa.com>

CompuServe: GO NCSA

E-Mail: info@ncsa.com

M. E. Kabay, Ph.D.

Director of Education, NCSA

Program Chair, CyberRisk '96



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 18: Issue 33

Weds 14 August 1996

Contents

- [Fault-tolerant software for escaping "upgrade hell"](#)
[Vladimir Z. Nuri](#)
- [RISKy cars coming!](#)
[Greg Dolkas](#)
- [128-bit Netscape registration](#)
[Alan Arndt via via Jim Horning](#)
- [Operator error or system design fault in Atlanta 911?](#)
[Philip Rose](#)
- [The 1994 A300-600 Nagoya accident - final report](#)
[Peter Ladkin](#)
- [Re: America Offline](#)
[Pete Mellor](#)
- [Re: Computers causing power outages](#)
[Robert I. Eachus](#)
- [Info on RISKS \(comp.risks\)](#)

⚡ Fault-tolerant software for escaping "upgrade hell"

"Vladimir Z. Nuri" <vznuri@netcom.com>

Fri, 09 Aug 96 13:04:28 -0700

The recent America Online blackout has spurred my thinking on the subject of decreasing the risks of software upgrades for real-time systems. I want to highlight for your readers some very significant techniques that I perceive to be underutilized to date and, if developed and used widely in the future, could hold great promise in drastically reducing the hazards of simple software upgrades. They are inspired by a maddeningly familiar pattern in software upgrades one might call "upgrade hell":

The fundamental difficulty we are observing in real-time software is that the system is often only designed to run one version of the software at a time. Designers are forced to bring "down" the system while they install new software, which may or may not function correctly. Often they can only test the full range of behavior or reliability of the new software by actually installing it and running it "live". Then, if the software fails to work, a process that in itself may be difficult to detect, they are forced to "down" the system again, and reinstall the old version of the software, if such a thing is even possible (in some cases the configuration of the new version is such that an older version cannot be readily reverted to).

This story repeats itself endlessly in many diverse software applications, from very large distributed systems down to individual PC upgrades.

In pondering this I came to some observations.

1. Many designers currently assume that new versions of software

will be

"plug-and-play" compatible with older versions.

2. Systems are designed to run one version of software at a time.

3. A system has to be inactive during transitions between versions.

4. Upgrades are only occasional and the downtime due to them is acceptable.

These basic features of software and hardware interplay, despite their wide

adherence, are not in fact "carved in stone". Could we imagine a directly

contrasting system in which they are fundamentally different?

1. Let us assume that new software is not necessarily compatible with

previous versions even where it should be, despite our best attempts to

make it so. In fact let us assume that humans are notoriously fallible

in creating such a guarantee and that in fact such a guarantee cannot be

realistically achieved.

2. Let us imagine a system in which multiple versions of software (at least

two) can be running simultaneously.

3. Let us imagine a system that "stays running" even during software version

upgrades.

4. Let us assume upgrades are periodic, inevitable, and ideally the system

would "stay running" even throughout an upgrade.

The above assumptions lead to some attractive properties of the whole I will

describe. One feature is similar to the way drives can be configured to

"mirror" each other, such that if either fails the other will take over seamlessly and the bad one "flagged" for replacement. Imagine now that computations themselves are "mirrored" in the hardware such that two versions of software are running concurrently, and the software checks itself for mismatches between the results of the computations where they are supposed to be compatible (this can be done at many different scales of granularity at the decision of the designer). The software could automatically flag situations in which the new code is not functioning properly, even while running the old version.

What we have is a sort of "shadow computation" going on behind the scenes.

When a designer wants to run a new version of software, he could "shadow" it behind the currently running software to test its reliability without actually committing to running it.

Under this new system, software upgrades tend to blend together:

- There is a point where only the old version is running.
- Then the old and the new version are overlapping or the new "shadowing" the old but the new not actually determining final results.
- Then reliability is actually measured, and continued to be measured until gauged sufficient.
- Finally, the actual commitment to running the new version alone can be made.
- Additionally, keeping around old versions that can be switched to immediately in times of crisis would be a very powerful advantage-- losing some new functionality but preserving basic or core functions.

There would be vastly fewer "gotchas" in this system than those

I outlined above in the classic "upgrade hell" scenario. Once the concept of different versions is embodied within in the software itself by the above principles, rather than it being considered foreign or external to the system, we have other very powerful techniques that can be applied:

A "divide and conquer" approach can be used to isolate bad new components. Different new components, all part of the new upgrade, can be selectively turned "on" or "off" (but still shadowed) to find the combination of new components that creates bad results based on the "live" or "on-the-fly" benchmarks of previous software. In fact, it may become possible to write software that actually automates the process of upgrading in which new versions of the components are switched on by the software itself based on passing automated reliability tests. The whole process of upgrading then becomes streamlined and systematic and begins to transcend human idiosyncracies.

These new assumptions could lead to radically different software and hardware systems with some very nice properties, potentially achieving what by today's standards seems elusive to the point of impossibility yet immensely desirable to the point of necessity: robust fault tolerance and continued, uninterrupted service even during software upgrades. Of course, the above techniques are inherently more difficult to achieve in implementation, but the cost-benefit ratio may be wholly acceptable and even desirable in many mission-critical applications, such as utility-like

services like telecommunications, cyberspace, company transactions, etc.

One difficulty of implementing the new assumptions above relative to software is that often such changes need to be made from the ground up, starting with hardware. But the software and hardware industries have shown themselves to be very adaptable to massive redesigns relative to new ideas and philosophies if they are shown to be efficacious in the final analysis despite some initial inconvenience, such as object oriented programming. I am not saying the above alterations are appropriate for all applications. They can also be introduced to varying degrees in different situations, ranging from a mere simplicity in switching between versions all the way to fully concurrent and shadowed computation with multiple versions immediately available.

Also, I am sure your astute readers can point out many situations in which the ideas I am outlining already exist. I am not saying they are novel. However the emphasis on them in a collection as a basic paradigm I have not seen before. In the same way that many designers were using OOP principles such as encapsulation, polymorphism, etc. before they were focused into a unified paradigm, I believe the above ideas could benefit from such a focused development, such as designing hardware, software, and languages that explicitly embody them. Many of the ideas I outline are used in software development pipelines and distinct QA/QC divisions of companies--

but I am proposing incorporating them in the machines themselves, which to my knowledge is a novel perspective.

Actually, the root concept behind these ideas is even more general than mere application to software. It is the idea that "the system should continue to function even as parts of it are replaced". We see that this basic premise can be applied to both hardware and software. It is such a basic attribute that we crave and demand of our increasingly critical electronic infrastructures, yet so difficult to achieve in practice. Isolated parts of our systems today have this property-- is it the case that it is gradually spreading to the point it may eventually encompass entire systems?

Many of these ideas come to me in considering a new protocol I am devising called the "directed information assembly line" (DIAL), a now-brief theoretical construct that supports such features, which I can forward to any interested correspondents who send me e-mail. Some of the key assumptions I am reexamining are those given above. I believe that actually changing our assumptions about the reliability of humans to be more lenient can actually improve the reliability of our systems. Let us start from new assumptions, including "humans are fallible", rather than "humans approach the limit of virtual infallibility if put under enough pressure" (such as that always associated with new versions and software upgrades).

V.Z.Nuri vznuri@netcom.com

⚡ RISKy cars coming!

Greg Dolkas <greg@core.rose.hp.com>

Tue, 13 Aug 96 15:52:22 PDT

In the 22 Jul 1996 issue of Fortune was an interesting look into the future of automobile electronics, "Soon Your Dashboard Will Do Everything (Except Steer)". The topic of steering has already been discussed in this forum, but what caught my eye was a review of the "OnStar" product from GM. Besides being a navigation aid, it also contains "some anti-bonehead features". These include the ability for you to call GM's "control center" for help if you lock your keys in the car, or forget where you parked it. >From the control center, they can "electronically reach into the car" to unlock the doors, or honk the horn and flash its lights.

Since the article doesn't discuss how the control center will authenticate that you really own the car you are asking them to unlock, or what measures are used to prevent a would-be control center from gaining access, it's not clear how the term "bone-head feature" should be applied...

Greg Dolkas greg@core.rose.hp.com

⚡ 128-bit Netscape registration

Jim Horning <horning@intertrust.com>

Wed, 14 Aug 96 12:21:00 P

>From: Alan Arndt
Sent: Wednesday, August 14, 1996 11:01 AM
To: Everyone!!
Subject: Your Privacy

While trying to download the 128-bit high-security version of Netscape, there was a notice about how they try to verify that you are a US Resident. Apparently they pass on the information you entered to another service and presumably if you don't show up you don't get to download the software.

That service is: <http://www.lookupusa.com/lookupusa/ada/ada.htm>
[[SHORTC~1.URL : 4620 in SHORTC~1.URL]]

I found this rather interesting. My name is not listed in most of these lists because they are usually based on phone numbers and mine is unlisted. This one, however, had my name and address, but no phone number. Not only that but it directly connects with a mapping service so you can get a direct map for the person's exact location. Quite neat, until you start to realize that it won't be long and people will VERY EASILY be able to find out a lot about you. Getting a map with an X on your house doesn't please me if someone is ticked off at me. Say they don't like my driving style on my motorcycle. (naw couldn't happen) Although personal information is no longer available from CA DMV I do believe you can get someone's Name from the license plate.

Now the Business lookup is even more fun. Not only can you map the location but you can get a Credit profile. Ours says Satisfactory. For \$3.00 you

can get the complete information.

Enjoy, and protect your valuable information.

-Alan

The following binary file has been uuencoded to ensure successful transmission. Use UUDECODE to extract.

```
begin 600 SHORTC~1.URL
M6TEN=&5R;F5T4VAO<G1C=71="E523#UH='1P.B\O=W=W+FQO;VMU<'5S82YC
; ;VTO;&]O:W5P=7-A+V%D82]A9&$N:'1M` `` `
`
end
```

⚡ Operator error or system design fault in Atlanta 911?

Philip Rose <phil.rose@zetnet.co.uk>

Tue, 13 Aug 1996 18:04:47 +0100

Last weekend the national press here in the UK published extracts from the police transcripts of the emergency traffic concerning the Atlanta bomb.

One thing that struck me was the operator's belief that the system's refusal to accept Centennial Park as a valid location was her fault. She even queried with the Police dispatcher whether she had spelled Centennial correctly.

I see two risks. Firstly, an overexpectation that a computerised system is error-free, and that every problem is operator error. Secondly, the deskilling of the operator's job increases the first risk.

Phil Rose Radcliffe, Manchester G3ZZA phil.rose@zetnet.co.uk

✶ The 1994 A300-600 Nagoya accident - final report

Peter Ladkin <ladkin@TechFak.Uni-Bielefeld.DE>

Wed, 14 Aug 1996 18:56:29 +0200

Aviation Week and Space Technology, 29 July 1996, pp36-37, contains the article "Pilots, A300 Systems Cited in Nagoya Crash" by Eiichiro Sekigawa and Michael Mecham, which summarises the final report of the Japanese Aircraft Accident Investigation Committee into the tail-first crash of China Air 140 into the runway at Nagoya on 26 April 1994, along with further information on the history of the A300 flight-control design for automatic/manual interactions.

Thus this accident has HCI aspects. It was discussed extensively in RISKS editions 16.05 (Stalzer), 16.06 (Wittenberg), 16.07 (Ladkin), 16.09 (Yesberg), 16.13 (Terribile), 16.14 (Ladkin, Overy), 16.15 (Shafer, Dorsett, Overy, Kaplow), and 16.16 (Dorsett, Ladkin, Kaplow, Mellor, Niland). The final report contains no surprises. Early rumors of a higher-than-expected blood alcohol level in the pilots (there is normally some found in autopsy, due to decomposition) and of an electrical power failure before the accident did not finally figure. All comments below within quotation marks "... " are quotations from Aviation Week.

The final report said that the crash was the result of the pilots fighting

the autopilot. It concluded that the pilots were inadequately trained in the "use and operational characteristics" of the autopilot. It also faulted Airbus Industrie's cockpit design, specifically the position of the autopilot's TOGA (takeoff/go-around) lever beneath the throttle; and "unclear writing" in the Flight Crew Operations Manual (FCOM).

The sequence of events was as follows. The First Officer (FO) was flying the approach to Nagoya, using the Flight Director (FD) and autothrottle, and accidentally triggered the takeoff/go-around (TOGA) lever (at time T), which is positioned just below the throttle levers. This caused the automatic flight system to go into 'go-around' (GA) mode: the FD issued 'pitch-up' commands. The captain noticed it, autothrottle was disengaged and thrust manually increased. Autopilots 1 and 2 were engaged (it's not clear why, perhaps in thinking to recapture the glideslope - the descent path - from which the aircraft had now departed), which didn't help since the AFCS was in GA mode. The aircraft was flying 18 degrees nose-up. The FO attempted for 20 seconds to force the nose down by pushing hard on the control column, thus 'fighting' the autopilot, which in response rolled in full nose-up trim to keep the pitch up. Finally, at T+45, the autopilots were disengaged, the captain took control. However, the alpha-floor protection triggered at T+50 from excessive angle-of-attack (that means that the aircraft was close to stalling) and brought in maximum thrust. However, this increased the nose-up attitude to over 52 degrees (since the wing was barely flying

because the airplane was by now so slow, the thrust generated a pitch-up moment about the horizontal axis through the wings, which was uncountered by aerodynamics at such a slow speed). The captain disengaged alpha-floor by retarding thrust, but the airplane had slowed to 78 knots, stalled at 1,800ft above the runway threshold, and crashed tail-first.

The cockpit voice recorder (CVR) shows the pilots were confused as to why the aircraft was not responding to the heavy manual nose-down command, despite C's recognising that GA mode had been engaged. The autopilot on all transport-category aircraft including this one can be manually disengaged by pushing the red autopilot-disconnect button on the handgrip of the control wheel. There is also an on/off switch on the cockpit forward control panel of A300/310 series aircraft which can be used to disconnect the autopilot.

The accident aircraft had automatic yoke-force disengagement of the autopilot inhibited below 1,500 ft AGL to avoid accidental disengagement of the autopilot during automatic landings. Airbus had already issued service bulletin SB A300-22-6021 recommending modification of the flight control computer (FCC) to allow disengagement by significant control column force above 400 ft AGL. China Air had not modified the accident airplane to SB A300-22-6021. Airbus "resisted changing its autopilot software below 400 ft. [sic] out of concern that pilots would have insufficient time to recover control if they inadvertently moved the yoke during an automatic

blind

landing." However, in March 1996 Airbus modified the system to deactivate below 400 ft. against yoke pressure of 45 lb. push and 100 lb. pull.

The Committee

- o said that alpha-floor combined with the unusual out-of-trim state in fact generated a heavy pitch-up moment, the opposite of what would be needed for stall recovery. It recommended that the BEA "study" this;
- o said that the captain misjudged the situation and should have taken over flight control earlier;
- o noted that Boeing and McDonnell-Douglas aircraft would have automatically disengaged the autopilot when heavy yoke forces were applied. "Their autopilots are also less likely to trim against pilot yoke inputs";
- o criticized Airbus for eliminating an audio alert for the stabilizer-trim-in-motion condition when the THS is in autopilot control. "Airbus should consider making the [...] sound in a THS out-of-trim condition, or if the THS moves continuously, regardless of autopilot engagement";
- o said Airbus needed "to study the function, mode-display and warning/alert system" in the current automatic flight-control system to "consider" pilot reactions. It concluded that the present system is too complicated in emergencies. "The BEA rejected this criticism";
- o called for Airbus to "improve" the FCOM instructions for manual override of the autopilot system, its disengagement in GA

mode,

and recovery procedures from an out-of-trim condition.

- o "was critical of Airbus" for not making modification SB A300-22-6021 mandatory in light of three similar incidents in 1985, 1989 and 1991;
- o recommended that manufacturers standardize specifications of automatic flight systems to make pilot training easier.

The US National Transportation Safety Board has accepted the findings of the report, as did Taiwan's Civil Aeronautics Administration (with only minor reservations). But the opinion of the French Bureau Enqu`etes Accidents differs in certain aspects, and the report includes a rebuttal of the BEA view.

The captain had over 2,600 hours in B747 and over 1,600 hours in A300-600 airplanes, as well as over 4,800 hours air force flight service. The FO had over 1,000 hours in the A300-600. Their behavior in fighting the autopilot, rather than disconnecting it (notwithstanding the yoke-force-disconnect on other airplanes); and in trying to force the airplane onto the ground (rather than going around and landing on the next try), remains simply incomprehensible to most pilots including this one.

More details and a fuller explanation of technical terms may be found under the Nagoya synopsis of my compendium 'Computer-Related Incidents and Accidents with Commercial Airplanes', accessible from <http://www.techfak.uni-bielefeld.de/~ladkin/>

Peter Ladkin

🔥 Re: America Offline (Cassel, [RISKS-18.31](#))

Pete Mellor <pm@csr.city.ac.uk>

Tue, 13 Aug 96 15:38:48 BST

In [RISKS-18.31](#), PGN added the footnote:-

```
>> [David, "dishonesty" sounds a little harsh. How well can
anyone
>> predict how long it is going to take to fix a problem that
has not
>> yet been identified and understood? PGN]
```

In response, in [RISKS DIGEST 18.32](#), "James K. Huggins" <huggins@eecs.umich.edu> writes:-

```
> Exactly. In fact, this is one of the oldest problems in our
field ... the
> fact that we don't know how to predict how long it will take
to do just
> about anything useful (write new code, fix an old piece of
code, etc.).
```

and smurf@noris.de (Matthias Urlichs) writes:-

```
> You can't, and that's the point. ...
```

I disagree. This view seems to be unnecessarily defeatist. What we are talking about here is measuring an attribute of a software-based system which is usually referred to as "maintainability" and can be defined quantitatively as "effort required to diagnose and fix a fault".

Software producers are in a position to measure this. (Whether they actually do or not is another matter.) The procedure to be followed would be something like the following:-

1. During the system trial (or beta-test), every failure is recorded
by the testers (or users) and reported to the design authority,
with all relevant data, such as symptoms and exception messages
observed at the time, memory dumps subsequently taken, etc.
2. The design authority then diagnoses the latent fault that was activated
and so gave rise to the failure. This would involve finding out:-
 - a) the location of the fault within the software,
 - b) the identity of the fault in terms of what exactly is wrong with the code, the module specification, or whatever,
 - c) the "trigger" conditions which activate the fault, and
 - d) a classification of the fault according to its cause (e.g., programming error, specification error, etc.) and effect (e.g., system crash, files corrupted, etc.).
3. The DA then devises a "fix", which might be a "work-around" to avoid the trigger conditions, or a modification to the software
to remove the fault permanently.
4. Regression testing is then required to ensure that the fix is effective, and that it does not introduce any new faults.
5. The effort (person-hours), overhead costs (e.g., machine time for regression testing), and elapsed time taken, are recorded for
each of these steps.

The result is a set of statistics (effort, cost and time to diagnose and fix each fault reported) which can be used as the basis for estimating effort, cost and time to deal with any fault reported during live use of the system.

Obviously, the effort, cost and time will vary, but a statistical analysis would yield useful figures such as mean time to repair

(MTTR)

and standard deviation, or median time to repair (MeTTR) with percentiles

(and similar statistics for cost and effort). The analysis could also break down the cost, effort and time by type, location, and severity of the fault.

Armed with this information, the producer is now in a position to make a sensible estimate of repair time, with confidence intervals, based on past data.

OK, this makes it sound simple, and I am fairly sure that few software

producers actually compile such statistics. (I would be very interested to

hear from any who do!) The best I could get (many years ago, for a support

team debugging large mainframe operating systems) was a vague statement from

the support manager to the effect that "My staff get through about three a week each."

However, if this seems odd, or unnecessarily onerous in terms of data

collection, bear in mind that it is quite normal for hardware equipment to

be sold with quoted mean time to failure (MTTF) and mean time to repair

(MTTR), with both of these statistics broken down to apply to particular

modes of failure. (In the hardware case, which widget has dropped off, and

how long does it take to find and fit a new one?) The reliability (measured

by MTTF), availability ($MTTF/(MTTF+MTTR)$) and maintainability (measured by

MTTR) are known.

[In the software case, there is a slight complication. Since software faults

tend to be transient (remove the trigger conditions and the

failure
condition goes away), the attribute "recoverability", measured
in terms of
"time to restore service", is of equal interest to
maintainability.
(Typically, you record and report the failure, reboot the
system, and carry
on working while the diagnosis and repair takes place off-
site.)]

As long as software producers are unwilling to make the necessary
measurements, then software development and support will
continue to remain
a "black art", and will not merit the term "software
engineering" in the
same way that we talk about "mechanical engineering", "civil
engineering",
etc.

Peter Mellor, Centre for Software Reliability, City University,
Northampton
Square, London EC1V 0HB, UK. Tel: +44 (171) 477-8422 p.
mellor@csr.city.ac.uk

✶ Re: Computers causing power outages (Hughett, [RISKS-18.32](#))

"Robert I. Eachus" <eachus@spectre.mitre.org>

Tue, 13 Aug 1996 18:27:03 -0400

> ... Not something that I want to hook my house up to.

Sorry about that, but your house is hooked up to it.

Philadelphia Electric

used to be pretty good about reserve capacity. (I haven't lived
there for

years, so I don't currently know.) However, what do you think
caused the

Great Northeast Power Blackout? What was obviously the real
cause of the

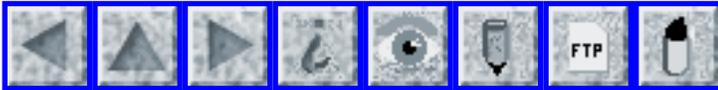
recent western blackouts? The interconnect grids are great if demand stays within bounds, but when heavily stressed they become amplifiers.

In the recent past politicians and financial analysts alike have been encouraging utilities to reduce their on-line excess capacity, and to shut down plants when not required for the current demand level. But excess capacity on-line is necessary to have a stable interconnect system. The difference in stability between 10 plants at running at of 81% capacity and 9 plants at 90% is dramatic. (If one facility has a glitch the network goes wild. It has just been thrown from stable operation into instantaneous overload, and at the best of times it will take the network hundreds of milliseconds--a dozen or so cycles--to stabilize. If transients cause generation facilities or transmission lines kick out before substations, the system is gone before any humans can react.)

The Northeast Blackout was caused by a coil failing in a relay in Niagara Falls. The relay had a backup coil which was energized immediately, and the main contacts never completely opened. In other words, the failover met specification. By the time the (amplified) voltage transient reached New York City, the result was spectacular, did damage in the tens to hundreds of millions of dollars, and killed a number of people. Some of you just saw a similar demonstration. Trying to figure out whether a fire in Idaho or a breaker tripped in California started the electric dominos toppling is detail. The important lesson is that if you run a grid too near

the edge it
amplifies fluctuations and imbalances. One glitch and we all
reap the
whirlwind.

Robert I. Eachus



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 18: Issue 34

Friday 16 August 1996

Contents

- [California DMV records NOT secure](#)
[Mark Seecof](#)
- [Re: London train crash: update](#)
[Scott Alastair](#)
[Jim Reid](#)
- [Re: 128-bit Netscape registration](#)
[Bernard Peek](#)
- [Re: Fault-tolerant software, "upgrade hell"](#)
[Kurt Fredriksson](#)
[Wayne Hayes](#)
[Valdis Kletnieks](#)
[Vladimir Z. Nuri](#)
- [Re: Electromagnetic pulses to stop car chases?](#)
[Michael Brady](#)
- [Re: Western Power Outage](#)
[Steve Forrette](#)
- [Re: America Offline](#)
[Valdis Kletnieks](#)
[Lowell Gilbert](#)
- [Re: Bread-riots and circuses](#)
[Hal Lockhart](#)

 [Info on RISKS \(comp.risks\)](#)

California DMV records NOT secure

Mark Seecof <Mark.Seecof@latimes.com>

Thu, 15 Aug 1996 12:26:37 -0700

I'd like to correct an oft-repeated misstatement; that California DMV records have been secured. In fact, quite minor procedural barriers to access by unsophisticated people at DMV counters have been instituted, but only slightly more savvy people can still get info, and the DMV continues to sell mass data extractions to reusers. Also, DMV has taken no steps at all to secure data or systems against misuse by DMV staff or others (e.g., police) with privileged access.

Re: London train crash: update ([RISKS-18.32](#))

"Scott Alastair (Exchange)" <ScottA@logica.com>

Tue, 13 Aug 1996 13:23:20 +0100

What happened was that a train from Euston to Milton Keynes with about 400 passengers on board was travelling North at about 60mph. Another empty train, which should have been waiting at a red signal just outside Watford Junction, started moving slowly South and crossed over a set of points onto the North-bound fast line straight into the path of the fast train. The fast train driver saw what was happening and sounded his horn but

could not avoid a collision. I believe that both drivers managed to jump clear before the crash and were not badly injured.

"Black boxes" were recovered from both crashed trains, and showed that signalling and train systems were working properly just before the crash. These black boxes, I understand, are a recent innovation and are not fitted to all trains.

It turned out that the crashed trains were both fairly new (about 10 years old) and had well-designed carriages which dissipated the force of the impact; also, that the collision was glancing and not head-on.

Newspaper photographs showed track torn up and the front carriages of both trains at crazy angles; one was hanging over an embankment. The other carriages of both trains were derailed but had not been thrown over. The line was closed for about 2 days while the carriages were removed and track repaired.

It was a huge stroke of luck that the collision involved new rolling stock: on some other lines carriages are 30 or 40 years old and are of an antique "slam-door" design which concertinas in the event of a crash. I have read that, of about 70 deaths on the United Kingdom railways in the past 10 years, all but one have occurred in these older carriages.

There are four separate enquiries going on at the moment - by Railtrack (who own the track), North London Trains (who own the trains), British Transport

Police and the UK Government's Health and Safety Executive - so I presume the reason for the supposedly stationary train moving will come out in due course.

Alastair Scott scotta@logica.com

✂ Re: London train crash: update ([RISKS-18.32](#))

Jim Reid <jim.reid@eurocontrol.be>

Tue, 13 Aug 1996 11:20:39 +0200

A number of risks have emerged from the recent crash. The first concerns Automatic Train Protection, ATP. This system is claimed to stop any train which passes a red signal. It is not used on the British railway network, though it is deployed on other European railways. [Apologies to any trainspotters for any simplification I've made.] The UK railway companies say that ATP is too expensive - it costs too much for each life it saves, though how they work that out is beyond me. (Another risk?) They claim that the money required for ATP would be better spent on other safety measures like modern, stronger passenger carriages. So, rather than prevent trains crashing into each other, they think the best strategy is to let them crash, but make the rolling stock safer. (Yet another risk?)

The next risk is the absurd way in which Britain's railways are now run after privatisation. One company - Railtrack - owns the stations, track and

signalling systems. It seems more interested in property development and turning stations into shopping malls than the rail infrastructure. This company would have to install ATP, which would make a big dent in their balance sheet. So, it's hardly surprising that they are not enthusiastic for ATP, even though they have some responsibility for safety. Railtrack charges train companies for the use of its stations and track. The train companies operate the services, but they don't own the rolling stock. These belong to leasing companies who hire them to the rail operators.

Aside from the bureaucracy and ticketing nightmares, there are serious safety risks in this setup. Safety of the trains is the responsibility of the leasing companies who own them and the operating companies who use them and presumably the companies who maintain them. Where the boundaries are is anybody's guess. Railtrack have responsibility for the safety of the track and signalling systems. However, if they were to deploy ATP, the leasing and operating companies would have to pay for the extra kit in the trains. Where the boundaries of responsibility lie between Railtrack and the leasing and operating companies is yet unknown. There was a recent report that a small fire was put out by staff throwing dirt and sand at the junction box. The box belonged to Railtrack, the staff worked for an operating company. They feared being disciplined if they used company property - their company's fire extinguishers - to help another company.

Sitting on top of this is a government agency, the Health and

Safety

Executive which is responsible for safety in the workplace amongst other things. Where their responsibility kicks in is yet another unknown. With no single body responsible for train safety, it's hard to apportion blame for crashes or establish better procedures and communications protocols to make them less likely in future. The companies and agencies involved end up shrugging their shoulders and pointing at each other.

An added problem is that none of these companies has safety as a prime objective. They all want to cut costs to boost their profits. For Railtrack, money spent on safety measures comes straight off their bottom line, reducing dividends for shareholders and profitability bonuses for management. For the leasing companies, repainting old trains is more cost effective than buying new ones which presumably have better safety features. For the operating companies, the cost of leasing is one of the few costs they can control. [They can also work their drivers harder, but that will be another safety risk.] Thus, they prefer to run old, less safe, trains because they are cheaper to lease than new ones.

✉ Re: 128-bit Netscape registration (Arndt, [RISKS-18.33](#))

Bernard Peek <bap@intersec.demon.co.uk>

Thu, 15 Aug 96 19:02:01 GMT

> Apparently they pass on the information you entered to another service and

> presumably if you don't show up you don't get to download the software.

That's quite interesting. Now what happens if I telnet into my other service provider (in California) and enter a perfectly valid name, US address and phone number.

Not that I would do it of course, it seems an unnecessarily convoluted way of achieving a fairly simple objective.

Risks readers might like to ponder a Catch 22 situation I found myself in some years ago. Working for a UK company selling high-tech equipment (68000 processors) I wasn't permitted to supply anyone on a blacklist. I could have been extradited and jailed for doing that. Of course I wasn't permitted to actually see the blacklist either.

And on another subject entirely...

> The final report said that the crash was the result of the pilots fighting
> the autopilot.

I've just heard a report of a crash that happened here two days ago.

It was a result of the two pilots fighting each other. As a result a business jet crashed on one of Europe's busiest roads. Four injuries, no fatalities.

Bernard Peek bap@intersec.demon.co.uk

✶ Re: Fault-tolerant software, "upgrade hell" (Nuri, [RISKS-18.33](#))

Kurt Fredriksson <etxkfrn@aom.ericsson.se>

Thu, 15 Aug 96 12:43:44 +0200

The author is right. This is not a novel idea. The Ericsson AXE exchange has had the functionality to upgrade software in a running system from the first system delivered more than ten years ago. This was a deliberate design decision due to the harsh demands on "uptime" in telecommunication systems.

Kurt Fredriksson

[Peter Denning reminds us that the Newcastle work on Recovery Blocks

-- Brian Randell et al. -- is relevant here, and certainly worthy of

mention. It goes way back to the mid 1970s. It was an extremely well

thought-out effort, with a language, a run-time system, and a supporting

hardware architecture for dealing with concurrent processes running

different versions of an algorithm (alternat[iv]e blocks), such that the

collection of processes would not terminate until at least one of them

passed an acceptance test. Their system include automatic checkpointing

so that you could back up properly to the last known state that passed an

acceptance test. Thanks to PJD for the reminiscence. PGN]

🔥 Re: Fault-tolerant software, "upgrade hell" (Nuri, [RISKS-18.33](#))

Wayne Hayes <wayne@cdf.toronto.edu>

Thu, 15 Aug 1996 00:27:25 -0400

"Vladimir Z. Nuri" <vznuri@netcom.com> writes about the possibility of running new software as a "shadow" of currently running software and (perhaps automatically) testing its reliability before switching it to "actively" controlling the system.

This method may be fine for bug fixes, but it has a fundamental limitation because it ignores a fundamental issue of software upgrades:

that the new software may have new functionality which is unavailable in the old version, and thus will never be tested while the old software is the only one that is "active".

For example, Bell Canada recently introduced phone mail to residences that previously only had "call answer". Since phone mail has fundamentally new functionality over call answer, the phone mail can not be tested under real-world conditions until its functionality is activated and actually used by the users. And if it fails, it will be difficult to reliably fall back to call answer alone, because then any phone mail messages left in the queue may be lost or left dangling.

✶ Re: Fault-tolerant software, "upgrade hell" (Nuri, [RISKS-18.33](#))

Valdis Kletnieks <valdis@black-ice.cc.vt.edu>
15 Aug 1996 17:03:22 GMT

I believe that the venerable Multics system supported this to some degree.

Also, IBM's AIX system has gotten quite good at update-on-the-fly (although

it's not *quite* up to full 24x7 yet), mostly due to the fact that most of the operating system kernel is loaded on the fly. There's still some gotchas, most notably in trying to reload a device driver after applying maintenance...

>What we have is a sort of "shadow computation" going on behind the scenes...

Unfortunately, if you have a system that's running at 85% capacity, you will require just about twice as much processor. Also, you introduce new failure modes. I believe the Space Shuttle uses a 5-way redundant system, with 4 systems made and programmed by one contractor, and the 5th a different design and programming from a separate contractor.

More than once, a shuttle launch has been scrubbed because the voting mechanism itself broke down.

On the other hand, I seem to remember that when the great long-distance telephone collapses happened a few years ago, a telco official was asked why they just don't reboot the switch, and he replied that this implied that the switches were booted a first time - apparently, some of them had been upgraded from mechanical rotaries through to several generations of more electronic and computerized designs, without ever actually going down..

Anybody have more info on how the telcos do software upgrades? They seem to have quite the good record on it (barring a few historical botches ;)

Valdis Kletnieks Computer Systems Engineer Virginia Tech

⚡ Re: fault-tolerant software for escaping "upgrade hell"

"Vladimir Z. Nuri" <vznuri@netcom.com>

Thu, 15 Aug 96 15:49:06 -0700

An nice analogy for fault-tolerant system upgrades struck me after I wrote the earlier article. When highways are being resurfaced, they are rarely barricaded entirely; instead traffic is diverted during off-peak periods and run at less-than-peak efficiency. I am trying to spur designers to think of the flow of data through programs as exactly the same kind of situation: ideally data could be easily rerouted through different parts of a system even as it is being upgraded. Of course, roads do not have the complexity of software-- the pavers do not have to worry about it not working properly once installed.

Kurt Fredrikson remarks that the "Ericsson AXE exchange" has the functionality to upgrade software on-the-fly. I am not familiar with it but I wonder if it has all the key properties I mentioned or if it subtly relies on any of the hidden "gotchas" such as assuming designers will infallibly carry over functionality between versions (i.e. no regressions). It is easy to claim that software can be instantly switched to a new version (or back to an old one), but such a mechanism is not entirely desirable without other features such as the ability to seamlessly compare the

compatibility results
of new versions with earlier ones.

In other words, one of my basic assertions in the essay is that regressions in software, where bugs in existing functionality are introduced in new versions, can be caught through more systematic methods than are generally being employed today. Wayne Hayes writes in a response that the system I propose cannot handle "new functionality". In the short essay I could not include this obvious caveat although it is quite apparent and a significant limitation. Actually, the essence of the mini-essay focuses on an elegant and graceful way of avoiding "regressions", and obviously one cannot have a regression when the functionality did not previously exist.

But Mr. Hayes also brings up an excellent related point about situations where new functionality conflicts with old functionality. In such cases designers could actually write code that "bridges" the two versions, such that they have fallback algorithms when the new code fails to function. In other words, they write a bit of additional code that tries to gracefully fall back or rearrange the system so that one can run the earlier version. Of course, that could have bugs too, and we tend to run into issues of infinite regress in some of these ideas. (Nevertheless, often companies have to assume that many of their software versions are running simultaneously.)

In fact there is a whole array of issues that readers can immediately spot-- this is exactly the kind of development and attention I suggest

be channeled
into creating computer languages and hardware systems that take
into account
all the various scenarios.

I want to highlight this point of Mr. Hayes'-- the system I am
describing
for graceful system upgrades is not designed to guarantee that
new
functionality is correct, only that old functionality is not
"clobbered" in
an upgrade, and no system downtime in the process. Of course
the process of
testing new functionality is an entire art form in itself.
However, because
"seamless software upgrading" does not guarantee the correctness
of new
functionality does not mean it is not superior to the systems we
have now,
which frequently do not even guarantee old functionality in
practice
(although the designers would insist they do in theory-- a
perception gap I
am explicitly challenging). If a new feature does not work
correctly but
the system is still running, that's highly desirable. Designers
would be
reluctant to be able to test new features without fear of breaking
the overall
system.

One nice way of thinking about this is the following: every
software package
is a core of functions, say $A = X + Z$. X is the core code that
should remain
compatible into the future. Z is code identified as obsolete and
"to be
deleted" in a future version. A new version, A' , adds some new
functionality Y , so that $A' = A + Y - Z = X + Y$. A "regression"
happens
whenever something in X fails to function in the new version,
something I am
suggesting can be better dealt with by a change in designer's

perceptions
and tools relative to the inherent evolutionary aspect of
software (in
contrast to the perception of inertness that holds today).

To summarize the above points in this framework, Mr. Hayes quite
rightfully
points out that if you don't have any prior information on Y,
the concept of
"regression" is not applicable. But also in his example, the
problem of
isolating exactly what Y is relative to X is apparent. Trying to
draw the
line between the two would be very difficult in some situations
such as the
case he gives, where new functionality is not merely an addition
on old
functionality but a replacement of aspects of it. However,
merely placing
attention onto the problem improves its chances for solution,
and the
designer is forced to explicitly answer the question, "how can I
gracefully
add this new feature and possibly revert to the old one if it
doesn't work?"

Mr. Kletnieks mentions another demand of graceful software
upgrading, that
if our system is running at anywhere over 50% capacity you would
have to add
capacity to mirror it if it is a real-time system. But to me
this is
essentially like describing mirrored disk drives to someone, and
them
saying, "but you have to have twice as many disk drives as you
now have".
That's the basic part of the cost/benefit tradeoff. Also, I
think that many
of the ideas can be used in non-realtime systems which would not
require an
upgrade in capacity but would instead imply slower running
times. Of course
there is additional overhead in introducing such ideas, just as

for example
in OOP the inherent overhead to function calls is increased due to the indirection. Of course, the power derived is inherent to this sacrifice.

The use of voting software in the space shuttle is one example of a system that is similar to what I am proposing. What he describes is essentially the idea of using shadowed computation on a single process to guarantee reliability, but the area of *upgrading* that I am focusing on is not as apparent in that example. Mr. Kletnieks' example makes a good point, however: the code designed to deal with multiple versions may itself have bugs in it. Again, the infinite regress-- what code will check the checker code? I suggest this will be less of a problem when the checker code is intrinsic to the language, so that this would be like asking the question, "what if the compiler has bugs in it"?

I would also like to point out that it ought to be up to the end-user to determine actual compatibility of versions. Today we have a system in which the companies that create the software give the assurance that it is or is not compatible, and the end-user often cannot determine whether this is so without committing to the new version, with the "upgrade hell" scenario frequently ensuing despite everyone's best intentions. In contrast, with a suitably flexible and powerful computation environment like I describe, it would be less relevant what the company promises, and the end-user could have ultimate control over testing and switching versions to match his own demands. How can a company guarantee it has a rigor in its

testing
environment that exceeds that of all its customers? History
generally
suggests they can't, and I suggest that systems be designed with
this in
mind, which give greater control to the end user in arbitrarily
and
seamlessly testing and switching between versions.

Based on responses, I am struck that the ideas I was
highlighting in my
original essay were explored somewhat thoroughly in the 70's,
yet they
apparently haven't made it into widespread use in software or
hardware. I
suggest they could be applied in varying degrees into areas
outside of the
incredibly demanding environments of telecommunications and space
exploration with fruitful results (I would also like to hear
more about how
telecommunication software is upgraded from RISKS readers-- the
infamous
AT&T switching disaster of a few years ago shows that it was
even "recently"
subject to catastrophic human miscalculations).

The graceful-upgrade paradigm seems to have failed to have made
the
difficult leap from theoretical curiosity to widespread use and
awareness by
"Joe Codehead". Again I think the analogy to OOP is relevant.
It took a
massive paradigm shift in consciousness for OOP to "trickle
down" throughout
the software industry. I suspect that the ideas for seamless
software
upgrades are roughly as significant and valuable and am writing
partly in
the hope others can take up this ideology for research and
implementation
beyond my own limited and minimal elucidations.

⚡ Re: Electromagnetic pulses to stop car chases? (Wayner, [RISKS-18.32](#))

Michael Brady <michaelb@gembok.corp.sgi.com>
13 Aug 1996 19:33:30 GMT

> Very precisely directed beams are required, ...

Of course the traditional car-stopping alternatives are a fusillade of gunfire, or a highly hazardous high speed pursuit, ramming of the fleeing vehicle, and, all too frequently, a "spirited arrest" by the pursuing officers. Except for the risk of turning pacemakers "up", "down", or "off", this non-lethal tool might be worth the collateral damage.

Michael Brady, CPP, Corporate Security Manager, Silicon Graphics, Inc.
Global Facilities, World Wide Administration Division
michaelb@corp.sgi.com

[Might as well try EMP (nuclear) while we are at it!
It would reduce traffic (but not congestion). PGN]

⚡ Re: Western Power Outage

Steve Forrette <stevef@wrq.com>
Tue, 13 Aug 1996 13:15:23 -0700

Regarding the power outage that hit several Western US states last Saturday, I had an interesting experience. I was in Las Vegas that weekend, and arrived at the Hilton hotel/casino where I was staying shortly after the

power outage started. At the time, I was unaware of the outage, and things appeared more or less normal inside, since the casino was on generator power. However, when I got to the front of the check-in line, I was told that I could not be issued a key to my room, since all of the machines that make the room keys (in this case, plastic cards with mag stripes) were "down." At first, they were sending new guests to their rooms accompanied by security, who would let them in with a master key. However, this quickly became overwhelming for them as the outage progressed, so they told us just to check back every 30 minutes until they got the card key machines working again.

With nothing better to do, I settled down in the bar :-), where I learned about the power outage. At this point, it was really interesting to see what Hilton considered essential enough to have on the backup generators, and what was "unessential" and therefore could be dark during the power outage. It was no surprise to see that *everything* on the casino floor was considered essential, right down to the chandeliers. Reportedly, everything went dark for a few seconds when the outage began and while the generators spun up. After that, whatever was on the backup system came back on. The slot machines remembered how many credits each player had, so at least that part of them must be on some sort of UPS.

In the bar, most of the lights were out, but the lights behind the bar, as well as all of the equipment needed to keep it open (beer and

soft drink
taps, cash registers, etc.) were on.

It was interesting that at the front desk, all of the computers were up, so they could check guests in and out, but the card key machines were not. The risk here is that even when you have a backup generator, your operations can still be crippled if you have a poorly thought out strategy of what you place on the backup system.

Steve Forrette, stevef@wrq.com

⚡ Re: America Offline (Mellor, [RISKS-18.33](#))

Valdis Kletnieks <valdis@black-ice.cc.vt.edu>

15 Aug 1996 17:19:51 GMT

The problem with this is that although it gives you a nice-looking set of graphs, it probably doesn't help you make any predictions until *after* you find and categorize the problem. All it *really* tells you is how long it takes to code various types of fixes.

When the system goes belly up, you probably can't right off the bat say "oh, that's a one-line error causing a memory overlay, 20 minutes to fix" or "We know what that is, it's a major design flaw that will take 4 man-weeks".

I once had to find a memory overlay in ISODE 8.0 (which is on the order of 500K lines of code). The error would only trip after about 6

million calls to the malloc() memory allocator, once about 120M of data had been allocated on the fly. Took me about 20 seconds to figure out "overlay". I then spent 3 80-hour weeks chasing it (we had a deadline to meet). Towards the end of the second week, I was becoming thoroughly convinced that the entire memory management system was trash and needed to be overhauled.

Final fix was 3 lines of C code, to repair where a programmer had forgotten to deal with one boundary condition.

I'm sure anybody who's been doing systems admin/support in the trenches for more than a few years has a whole collection of horror stories where the initial diagnosis had absolutely no relationship to the actual problem....

Valdis Kletnieks Computer Systems Engineer Virginia Tech

✉ Re: America Offline (Mellor, [RISKS-18.33](#))

Lowell Gilbert <lowell@epilogue.com>

Fri, 16 Aug 1996 08:29:33 -0400

Pete Mellor claims (in [RISKS-18.33](#)) that if software producers/maintainers keep better records, they'll become Real Engineers and be just as able to accurately predict the "effort required to diagnose and fix a fault" as other kinds of Real Engineers.

While I wouldn't remotely suggest that better measurements couldn't improve predictability, truly accurate estimates of time to fix a bug

that's not yet understood will always be an unachievable goal. The metaphor of hardware design, although tempting because software designers tend to work closely with hardware designers, is so weak as to be downright disingenuous. Software *is* different from hardware in some very relevant ways, but the most critical for this discussion is the fact that every bug is different. You can measure mean-time-to-failure for a light bulb quite accurately, but that's because every light bulb failure is the same. Every software problem, however, is unique. [to paraphrase Tolstoy] Once a software bug is fixed, it shouldn't occur again in the (repaired) code base.

You can make predictions of service intervals extremely precise by collecting enough data about previous problems. However, they will be no more accurate than the similarity between the problems. The RISK, as usual, is that the world will unexpectedly be more complicated than our model of it. [The key word being "unexpectedly." Of *course* the world will be more complicated than the model. That's the *purpose* of making a model.]

✉ Re: Bread-riots and circuses (O'Connell, [RISKS-18.32](#))

Hal Lockhart <hal@platsol.com>
Thu, 15 Aug 1996 11:34:25 -0400

This reminded me of a true situation that I remember reading about a while

back (1980's?). In some city in the Mideast (Beirut?), there was fighting in the streets every night. But one night a week there was peace, because everyone stayed home to watch two episodes of Kojak broadcast one after the other by two different TV stations. The locals named the phenomenon "double Kojak".

Harold W. Lockhart Jr., Platinum Solutions Inc., 8 New England Executive Park, Burlington, MA 01803 USA hal@platsol.com (617)229-4980 X1202

[From hijack to lojack by Kojak? Here is an opportunity for pacifist Trojan horses: distributing highly addictive interactive computer games to both sides. 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 18: Issue 35

Monday 19 August 1996

Contents

- [Justice's Web Site Is Infiltrated](#)
[Edupage](#)
- ["Vandalized" nuclear controls - Florida](#)
[Howard Goldstein](#)
- [The risk of plagiarism with Websites \(Roy Dictus\) Names of punctuation as a risk](#)
[Jeremy J Epstein](#)
- [Inability to "take it apart and see how it works"](#)
[Daniel P. B. Smith](#)
- [Reliance on e-mail in an emergency](#)
[Ramon L. Tate](#)
- [The Atlanta 911 transcript](#)
[PGN](#)
- [Buggy metaphors](#)
[William Ehrich](#)
- [How telcos upgrade switches](#)
[R. Spainhower](#)
- [Rebooting vs. 7x24 Operations](#)
[Jeremy Leader](#)
- [Re: Upgrade Hell](#)
[Henry G. Baker](#)

- [Measuring time-to-fix](#)
[David Holland](#)
 - [Alternatives to Social Security Numbers](#)
[Robert Ellis Smith](#)
 - [Re: Department of Motor Vehicle records](#)
[Jan Vorbrueggen](#)
 - [Re: California DMV records NOT secure](#)
[A.E. Siegman](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ **Justice's Web Site Is Infiltrated (Edupage, 18 August 1996)**

Edupage Editors <educom@elanor.oit.unc.edu>
Sun, 18 Aug 1996 16:12:13 -0400 (EDT)

The U.S. Justice Dept.'s Web site < <http://www.usdoj.gov/> > took on a quite different look after crackers broke in this weekend and altered the page to include swastikas, obscene pictures and criticism of the Communications Decency Act. The site was shut down following the discovery Saturday morning; the department expects to reconstruct the page and have it running again by Monday, if not before. (*St. Petersburg Times*, 18 Aug 1996, A12)

⚡ **"Vandalized" nuclear controls - Florida**

Howard Goldstein <hgoldste@mpcs.com>
17 Aug 1996 18:18:30 GMT

The FBI pulled out of an investigation concerning glued switches discovered

in a backup control room at FPL's Hutchinson Island (near Ft
Pierce,
Florida) nuclear facility, so reports the AP in an item carried
in 16
August's *_Florida Today_*.

A security alert was issued Wednesday when glue was discovered
in three
locked switches in the backup control room, a facility used in
case the
primary control room is unusable. An FBI spokesman is quoted as
justifying
pulling out of the investigation because the FBI lacked
"jurisdiction...it
really came down to an act of vandalism or tampering."

The piece fails to mention the plant features that would have
been affected
by the glued switches.

Investigation is reportedly focused on employees. The article
implies
a link between the vandalism and complaints about a November
round of
job cuts at the facility.

⚡ The risk of plagiarism with Websites

"Roy Dictus, NET" <roy@net.be>
Wed, 14 Aug 1996 00:03:42 +0200

My company recently got ripped off by a competitor. We build
Websites and
thus had constructed a site detailing our products and services.

A rival Website constructor (!) copied practically the entire
site,
changing the background color, changing our name into theirs,
and making
other slight changes like alignment, add and delete a word or

phrase
here and there...

I complained about it, not only to them directly, but also on a local USENET newsgroup (we're both located in Belgium, so the newsgroup was be.providers).

On the phone they just laughed at me and admitted to copying, but on USENET they claimed I had copied their site!

There's nothing I can do to prove them wrong, even though we both know what happened.

The risk: if you put your materials on the Internet, where they can be freely copied, make sure you have some way to prove you made them yourself, and when you did it.

Roy Dictus, NET bvba, Internet Projects & Consulting
roy@net.be <http://www.net.be>

[Interdictus becomes Enter Dictus. PGN]

⚡ Names of punctuation as a risk

JEREMY J EPSTEIN <JEPSTEIN@cordant.com>
Fri, 16 Aug 1996 16:21:37 -0500

My sister in Israel recently joined the Internet. She had a certain amount of trouble getting her PC configured correctly to hook to the service provider, in part because (I'm told) the name of the semicolon in Hebrew is

(translated) "period comma". So when she was told over the phone to put in a "period comma" in a configuration file, she did that (.,) rather than the required semicolon (;). Needless to say, the software didn't find the two interchangeable.

I think the risk is that we computer-types assume that everyone will understand the ambiguous meaning of terms. The fact that this happened to be in another language just makes the point a bit clearer.

✶ Inability to "take it apart and see how it works"

"Daniel P. B. Smith" <dpbsmith@world.std.com>
Sat, 17 Aug 1996 16:28:09 -0400 (EDT)

When my father was nine, his Uncle Will, who was fond of practical jokes, gave him a magnetic compass--and said "Why don't you take it apart and see how it works?"

Technical education rests on intuitive understanding gained through unsupervised, unstructured exploration in childhood. Before I went to MIT, I was crushing vacuum tubes in vises, and connecting automobile spark coils to a big antenna to see whether my friend with the shortwave radio could pick up the resulting RFI. [...]

Thirty years ago, a lot of our technology was accessible to direct exploration. You could "take it apart to see how it works." You could see the grooves in a phonograph record, put it under a microscope

and see the wiggles, and experiment by putting fingernails or sharp objects into the grooves. You could smash a vacuum tube and see the little grid wire inside it. You could overload a vacuum tube and see the anode get red hot. (My real learning took place in the basement, not the science fair).

What is the effect on our society as more and more of our technology vanishes inside the chip? The behavior of engineered objects depends less and less on physical and mechanical relationships, and more and more on arbitrary behavior designed into firmware. I fear that the engineers of the future will lack a certain kind of gut intuition that comes from direct tactile contact with "the works." We know what is being gained, but are we sure we know what is being lost?

Daniel P. B. Smith dpbsmith@world.std.com

✶ Reliance on e-mail in an emergency

Ramon L. Tate <rtate@helix.nih.gov>

Mon, 19 Aug 1996 11:07:42 -0400

As did many organizations, the National Institutes of Health received several bomb threats on Monday, July 29, in the wake of the bombing in Atlanta, GA. Several buildings were evacuated and searched but no bombs were found. While the NIH campus is extensively networked, the use of e-mail as a general notification mechanism was found to be wanting:

[excerpted from a memo from the NIH Director]

"In addition to notification of all staff through usual administrative channels, an attempt was made soon after the threats were received to utilize our e-mail system to inform all NIH staff of the threats. The delivery of this notification was delayed in many cases because an equipment failure over the weekend created a backlog of messages on Monday morning and because our current list-serv system was unable to deliver 24,000 messages in a timely fashion."

This incident serves to underline the oft-stated (and oft-ignored) risk in relying on systems that were (a) not designed to do the job required of them and (b) never subjected to realistic testing to see if they *could* do it anyway.

Ramon L. Tate, Ph.D., National Institutes of Health, Bldg.14A,
Rm. A116
Bethesda, MD 20892-5515 rt3e@nih.gov

The Atlanta 911 transcript

"Peter G. Neumann" <neumann@csl.sri.com>
Fri, 16 Aug 96 10:45:34 PDT

[The following transcript of the Olympic 911 bomb call and the ensuing conversation suggests that many of our nontechnological risks are not being adequately addressed. PGN]

<http://www.cnn.com/US/9608/09/olympics.bomb.911/911.transcript.wir/transcript.html>

Excerpts from a transcript released Thursday by the Atlanta Police Department regarding the bomb threat telephoned to 911 on July 27. Times have been converted from military time to standard notation, and punctuation and spelling have been edited. Parenthetical notes are part of the police transcript except where labeled as an editor's note.

The transcript refers to these police terms: Code 73, bomb threat; and Zone 5, a police precinct near Centennial Olympic Park.

The transcript did not explain the Zone 5 dispatcher's references to Code 17 and Code 8, which apparently were unrelated to the bomb call.

12:58:28 a.m.: [Call to 911]

12:58:32 a.m.: Atlanta Police Department 911 Operator: "Atlanta 911."

Caller: "There is a bomb in Centennial Park, you have 30 minutes."

12:58:45 a.m.: Caller hangs up.

1:01:20 a.m.: 911 operator calls APD Agency Command Center (all lines busy).

....

1:01:30 a.m.: 911 operator calls Zone 5 and notifies Zone 5 of Signal 73 and requests address of Centennial Park -- unable to get street address.

Dispatcher: "Zone 5."

911 Operator: "You know the address to Centennial Olympic Park?"

Dispatcher: "Girl, don't ask me to lie to you."

911 Operator: "I tried to call ACC but ain't nobody answering the phone ...
but I just got this man called talking about
there's a
bomb set to go off in 30 minutes in Centennial
Park."
Dispatcher: "Oh Lord, child. One minute, one minute. I copy
Code 17. OK,
all DUI units are Code 8 and will not be able to
assist on the freeway.
Oh Lord, child. Uh, OK, wait a minute, Centennial
Park, you put it in and it won't go in?"
911 Operator: "No, unless I'm spelling Centennial wrong. How
are we spelling
Centennial?"
Dispatcher: "C-E-N-T-E-N-N-I -- how do you spell Centennial?"
911 Operator: "I'm spelling it right, it ain't taking."
Dispatcher: "Yeah."
911 Operator: "Centennial Park is not going. Maybe if I take
'park' out,
maybe that will take. Let me try that."
Dispatcher: "Wait a minute, that's the regular Olympic
Stadium right?"
911 Operator: "Olympic Stadium is like Zone 3, though.
Centennial Park."
Dispatcher: "That's the Centennial Park?"
911 Operator: "It's near the Coca Cola Plaza, I think."
Dispatcher: "In 5?"
911 Operator: "Uh huh."
Dispatcher: "Uh, hold on. Sonya, you don't know the address
to the
Centennial Park?"
2nd Dispatcher (in background): "Downtown."
911 Operator: "Male, about 30."
Dispatcher: "1546, Code 17, 23."
911 Operator: "White."
Dispatcher: "Uh, you know what? Ask one of the supervisors."
911 Operator: "No, Lord help me, you know they don't know."
Dispatcher: "I know, but it gets it off you."
911 Operator: "Alrighty then, bye."
Dispatcher: "Bye."

1:02:40 a.m.: 911 operator calls APD ACC for address

(telephone line problem;
operators cannot hear each other.) ...

1:02:50 a.m.: 911 operator calls APD ACC again and requests
address for
Centennial Park and is given the telephone
number.

ACC: "Atlanta Police, Agency Command Center."

911 Operator: "Hey, can you hear me now?"

ACC: "Uh huh."

911 Operator: "OK, can you give me the address of the
Centennial Park?"

ACC: "I ain't got no address to Centennial Park, what
y'all
think I am?"

911 Operator: "Can you help me find the address to Centennial
Park?"

ACC: "I can give you the telephone number of
Centennial Park."

911 Operator: "I need to get this bomb threat over there to
y'all."

ACC: "Well."

911 Operator: "But I need the address of Centennial Park. It's
not taking,
the system is not taking Centennial Park, that's
not
where it came from, but you know the system is
not
taking Centennial Park, that's where he said the
bomb was."

ACC: "No particular street or what?"

911 Operator: "He just said there's a bomb set to go off in 30
minutes in
Centennial Park."

ACC: "Ooh, it's going to be gone off by the time we
find the
address."

911 Operator: "Are you kiddin'? Give me that, give me that."

ACC: "I mean I don't have an address, I just have
phone
numbers."

911 Operator: "Give me the phone number."

...

1:05:10 a.m.: 911 operator calls Centennial Park for street address and
is placed on hold. Receives address at 1:07:10 a.m.

Centennial Park: "Centennial Park, this is Operator Morgan."

911 Operator: "Hi, can you give me the address to Centennial Park?"

Cen Park: "The address?"

911 Operator: "Uh huh."

Cen Park: "Uh, hold on a second."

1:06:30 a.m.: 911 operator notifies Communications Supervisor, Sgt.

Montgomery.

911 Operator: "Does anybody -- Sgt. Montgomery, do you know the address of

Centennial Park? Do you know the address to Centennial Park.

Well, I need to get the address of Centennial Park 'cause, I

mean I don't mean to upset nobody, but we got a bomb threat

over there."

(Editor's note: The transcript does not further indicate whether this

comment about a bomb threat was directed only to Sgt. Montgomery in the

911 center or to Centennial Park's Operator Morgan, who is shown to come

back on the line just after the comment.)

Cen Park: "Ma'am."

911 Operator: "Yes."

Cen Park: "OK, it's 145 International Boulevard."

911 Operator: "145 International Boulevard."

Cen Park: "Uh huh."

911 Operator: "OK."

Cen Park: "All right, uh huh."

911 Operator: "Thank you. Bye bye."

1:08:35 a.m.: 911 operator sent call to dispatch.

1:11:10 a.m.:

Dispatcher: "1591. Radio raising 1594."

Unit 1594: "1594. You call?"

1:11:20 a.m.:

Dispatcher: "1594, that's affirmative, got a Signal 73 at 145 International Boulevard. It came from the pay phone at the Days Inn. The caller is advising that he has one set to go off in 30 minutes at Centennial Park. Sounded like a white male."

(Editor's note: The same information is then given to Unit 1593 and the dispatcher calls Unit1546.)

1:12:30 a.m.:

Dispatcher: "Did you copy?"

1:12:40 a.m.:

Unit 1546: "1546. I copy. Advise the state police, they police that park.

I'll go the Days Inn and see if I can locate the caller."

Dispatcher: "OK, that's affirmative."

(Editor's note: There are sporadic entries over the next seven minutes.

Another officer, designated Unit 1593, also instructs the dispatcher at

1:18:50 a.m. to "contact the state police supervisor." The transcript

contains no indication, however, that state police were notified.)

1:20:00 a.m.:

Unit 2924: "2924 to Radio, be advised that something just blew up at

Olympic Park."

✂ Buggy metaphors (Gilbert, [RISKS-18.34](#))

William Ehrich <ehrich@minn.net>

Sun, 18 Aug 1996 09:32:16 -0600

Lowell Gilbert wrote in [RISKS 18.34](#):

> The metaphor of hardware design ... is so weak as to be downright disingenuous.

A better metaphor might be crime. It is hard for a detective to predict accurately how long it will take to find out who committed a crime. It is equally hard to prevent future crimes. And we've been trying to solve those problems for much longer than we have been debugging software.

- Bill E

✂ How telcos upgrade switches (Kletnieks, [RISKS 18.34](#))

<rs@world.std.com>

Mon, 19 Aug 1996 10:45:48 -0400

Bruce Sterling provides a very interesting summary of how the telephone companies take care of software upgrades to switching systems in his book [_The Hacker Crackdown_](#).

The basic process is this: start with all of the switching stations with the old software. Outfit one station with the new software. Watch it run for a while and see what happens. If it's broken, only a few (!)

people will be out of phone power. When it seems like it's working OK, add another station. When that one seems like it's working, add another station. And so on until all of the switches are outfitted with the new software.

The legendary Crash of 1990 happened when AT&T had approximately 75% of stations outfitted with new software, and the bug that caused the crash could only cause a crash when a critical mass of stations had the new software (and the new bug).

R. Spainhower

rs@world.std.com

⚡ Rebooting vs. 7x24 Operations

Jeremy Leader <jeremy@worlds.net>

Fri, 16 Aug 1996 13:44:18 -0700

The recent discussion of seamless upgrades, and the idea that telephone switches might never have been "booted" to begin with (having been seamlessly upgraded over the years from their original mechanical incarnations) reminded me of a similar situation.

This was when I worked for a large mainframe manufacturer (the adjective applies to both the company and their products) in the mid-1980s. I was working with the folks who wrote the operating systems for these mainframes, and we had roughly half a dozen machines used by various software development projects (OS, compilers, databases, tools, etc.). Many of these machines were running early beta test versions of the operating

system.

These machines could either be "cold booted", where a fresh operating system image was loaded from tape to disk and various data structures on the disk re-initialized, or "warm booted", where the current operating system image was used, with the data structures as they were when the machine was stopped. Patches could be (and frequently were) applied to the operating system image on disk, followed by a warm boot.

It turned out that no one was cold-booting the machines, because it took too much time and effort. It was discovered that some machines hadn't been cold-booted for many months! Typically, in that time, dozens of patches had been installed, some of which might affect the cold-boot process. Management announced that all machines would henceforth be cold-booted weekly, to verify that they still could be.

The risk of a system that almost never needs to be taken down is that when it does need to be taken down, it might be hard to bring it back up! Or, practice makes perfect?

Jeremy Leader Tujunga, CA, USA jleader@alumni.caltech.edu
<<http://www.alumni.caltech.edu/~jleader/>>

✉ Re: Upgrade Hell (Nuri, [RISKS-18.33](#))

Henry G. Baker <hbaker@netcom.com>
Sat, 17 Aug 1996 09:17:04 -0700 (PDT)

1. Upgrading a program is usually pretty easy -- the hard part

is upgrading the database it operates on. It's amazing that 'program development environments' spend all this effort on the program portion, and virtually none on the database portion. Common Lisp Object System (CLOS) is one of the few systems that actually provides a smooth 'upgrade' mechanism in which multiple versions of objects can simultaneously coexist, along with a 'lazy upgrade' ability -- older objects can be automatically upgraded 'on sight'.

2. Without rehashing all of the arguments for/against N-version again, I just want to point out a few key ones against. There are occasions where any decision is better than no decision -- e.g., which side of an obstacle to detour around; it usually doesn't matter, but you are guaranteed to crash if you don't choose one. Apparently, at least one crash (or near-crash) of an experimental, statically-unstable NASA airplane occurred when two different systems proposed two different answers, and the supervisor system concluded that both subsystems must have malfunctioned, thus causing the big red light on the pilot's console to come on ("total computer system malfunction") (heresay from a conference lunch conversation). Another problem from the multiple language N-version efforts (C/Fortran/Ada): a good answer from -- e.g. -- the Ada implementation can be outvoted by a bad answer from -- e.g. -- the C and Fortran implementations.

Henry Baker <ftp.netcom.com:/pub/hb/hbaker/home.html>

✂ Measuring time-to-fix (Mellor, America Offline, [RISKS-18.33](#))

David Holland <dholland@hcs.harvard.edu>

Mon, 19 Aug 1996 20:43:13 -0400 (EDT)

Several people have made the point that you can't classify bugs in advance of fixing them and therefore can't make much in the way of useful predictions of how long it will take to fix them.

This is quite true (although some very vague generalizations can be made.)

It would be more interesting, however, to measure the time it takes to fix bugs in particular programs. Some programs are better designed than others. Some of the time this translates into some programs being more debuggable than others. (And sometimes it doesn't.) There are thousands of other factors involved, but I suspect most of them are reasonably uniform for the lifetime of a single project at a single company.

Thus you might be able to make some vague predictions for the time it takes for the average bug in a specific program (well, code base, probably) to be fixed.

Admittedly this is not especially useful for telephone companies and the like, but it might work for an operating systems vendor. Or for customers choosing software, if vendors could be convinced to disclose the data.

One would have to get some actual data to see if any statistically useful conclusions can be drawn.

David A. Holland dholland@hcs.harvard.edu

✶ Alternatives to Social Security Numbers

Robert Ellis Smith <0005101719@mcimail.com>

Fri, 16 Aug 96 15:24 EST

Last spring, I asked readers of RISKS for suggestions on alternatives to Social Security numbers in organizations with large data bases of information about individuals. Many such organizations find they do not need to use SSNs, and avoid privacy problems associated with using them. For a copy of all of the responses, send a request to us and specify whether you want hard copy or electronic edition of our August issue, and provide postal address or e-mail address.

Robert Ellis Smith, Publisher, Privacy Journal newsletter, Providence, RI, 401/274-7861, e-mail 5101719@mcimail.com.

Excerpts from the suggestions follow:

* FROM WASHINGTON, D.C.: Maryland uses Soundex (of name and birth date concatenated [linked in a chain]) both for driver and vehicle registrations.

* FROM CAMBRIDGE, MASS.: "Against Universal Health-Care Identifiers" in the JOURNAL OF THE AMERICAN MEDICAL INFORMATICS ASSOCIATION 1:316-319, 1994, by Dr. Peter Szolovits of MIT and Dr. Isaac Kohane of Children's Hospital in Boston, discusses a number of ways in which cryptography-based health care

identifiers can be used to preserve privacy while remaining manageable for typical medical purposes. This is publication #49 (in Postscript format) at <http://medg.lcs.mit.edu/people/psz/publications.html>.

* FROM YARDLEY, PA.: One way is to use a simple scheme like three letters from last name, the first initial, and some digits; another is just to use sequential numbers. Another is an MD5 hash of the full-name string [a one-way mathematical function as a stand-in for the name that makes translation back to the original name impossible]. This is always unique for a unique string, so you might need to add some numbers.

* FROM MADISON, WISC.: When I was working on the development of the Wisconsin Student Data Handbook - we tried to develop what we called an "SSN surrogate," also of nine bytes per individual. It involved an algorithm which combined year, month, and date of birth with sex and two consonants each extracted from the first and middle names.

* FROM CYBERSPACE: I worked with a banking software company that set up employee records simply by exact hire date and time. Since they never hired anyone at exactly the same time, it gave each person a unique number. You could do the same for any data base in which records are added gradually one at a time - just number them based on exact date and time added.

* FROM PALO ALTO, CAL.: At Stanford University we made a decision long ago not to use SSN for identification except where required by law (payroll taxes, for example). We use a unique Stanford University ID (SUID), which is a lifetime number and applies to all students, alumni,

faculty, staff,
and patients. It serves all the same purposes that the SSN
would do if it
were used.

✉ Re: Department of Motor Vehicle records (Johnsrude, [RISKS-18.31](#))

Jan Vorbrueggen <jan@fsnif.neuroinformatik.ruhr-uni-bochum.de>

Mon, 19 Aug 1996 13:12:06 +0200

Johnsrude writes:

> This lack of protection distinguishes American law from most
European
> democracies. "Data protection" is an important part of
European human
> rights law.

A very important point. In Germany, this was actually derived,
in the
context of a census, from the constitutional right to freedom
from injury by
the Bundesverfassungsgericht (sort-of-analogue of the US Supreme
Court). The
laws that were made in response to this decision actually strive
to handle
the problem at the correct point, IMO, namely when the data in
question is
created. And there is a distributed system of "watch dogs"
whose annual
reports are widely discussed (if not always read).

However, I think the bulk of Johnsrude's contribution and the
further
discussion in this thread misses a major point. The DMV database
is quite
different from, say, VISA's or your favourite retailer's, in
that the DMV

occupies a monopoly, and a publicly mandated one at that. If you don't like the data handling procedures of whoever offers you a service, in general there will be a competitor who might have better practices regarding your objections. Or you can make a purchase explicitly contingent on data concerning it not being made available to others, and in the case of infraction sue for breach of contract (of course, this entails other barrels of worms, but that's a separate discussion). In the case of the DMV, there is no alternative, because the DMV itself, as an issuer of drivers' licenses, serves a public watchdog function, and the service it offers is not in any practical sense optional, especially in wide parts of the United States. Putting severe restrictions on the DMV's use of the data entrusted to it is sensible, for any number of reasons; the technical problems in distributing data to those that need to know (e.g., police officers) come up in other situations as well and have well known solutions.

One of the root problems here is that, IMHO, the way legislative responsibility has been divided in the USA is just crazy. The (I assume) federally mandated inclusion of the SSN in state controlled DMV records, without any clauses on how to protect this data, is a case in point; I suppose this was foisted on the states in a similar way the drunk driving rules were (according to urban legend, by making federal subsidies for the interstates contingent on such legislation). Thus, responsibility is divided - in a similar way later noted as being the result of the privatization of

the British rail network.

Jan

⚡ Re: California DMV records NOT secure (Seecof, [RISKS-18.3x](#))

AES <siegman@ee.stanford.edu>

Fri, 16 Aug 1996 15:52:22 -0700

Not to hammer this point, but if DMV records are going to be readily and speedily available to law enforcement agencies at the lowest level, e.g., deputy sheriffs and dispatchers in the smallest communities, as seems necessary to me for rational police work, then as a practical matter these records are not secure at all, at least not to any intruder with a modicum of intelligence..

The RISK of thinking that DMV records are secure when in fact they're not then seems worse to me than the benefits, if any, of thinking they are secure.



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 18: Issue 36

Weds 21 August 1996

Contents

- [Internet Explorer Security Problem](#)
[Ed Felten](#)
- [Computer Testing of Nuclear Weapons](#)
[Frank C. Ferguson](#)
- [Swiss address risks of holding referenda by Internet](#)
[PGN](#)
- [Risks of remote-controlled fireplaces](#)
[Jeffrey Mattox](#)
- [Re: Escaping software upgrade hell](#)
[Vladimir Z. Nuri](#)
- [Re: London Train Crash](#)
[Roger Hird](#)
[Clive D.W. Feather](#)
[Martin Poole](#)
- ["Authentication Systems for Secure Networks" by Oppliger](#)
[Rob Slade](#)
- [Info on RISKS \(comp.risks\)](#)

⚡ Internet Explorer Security Problem

Ed Felten <felten@CS.Princeton.EDU>

Wed, 21 Aug 1996 13:12:59 -0400

We have discovered a security flaw in the current version (3.0) of Microsoft's Internet Explorer browser running under Windows 95. An attacker could exploit the flaw to run any DOS command on the machine of an Explorer user who visits the attacker's page. For example, the attacker could read, modify, or delete the victim's files, or insert a virus or backdoor entrance into the victim's machine. We have verified our discovery by creating a Web page that deletes a file on the machine of any Explorer user who visits the page.

The core of the attack is a technique for delivering a document to the victim's browser while bypassing the security checks that would normally be applied to the document. If the document is, for example, a Microsoft Word template, it could contain a macro that executes any DOS command.

Normally, before Explorer downloads a dangerous file like a Word document, it displays a dialog box warning that the file might contain a virus or other dangerous content, and asking the user whether to abort the download or to proceed with the download anyway. This gives the user a chance to avoid the risk of a malicious document. However, our technique allows an attacker to deliver a document without triggering the dialog box.

Microsoft has been notified and they are working on fixing the problem.

Until a remedy is widely available, we will not disclose further

details
about the flaw.

For more information, contact Ed Felten at felten@cs.princeton.edu or 609-258-5906.

Dirk Balfanz and Ed Felten
Dept. of Computer Science, Princeton University
<http://www.cs.princeton.edu/sip/>

✶ Computer Testing of Nuclear Weapons

"Frank C. Ferguson" <ferguson@dma.dma.org>
Tue, 20 Aug 1996 16:37:09 -0400 (EDT)

An AP dispatch out of Washington reported that IBM has won a government contract to build the world's most powerful computer -- an ultrasupercomputer that is 300 times faster than any machine now in use. Energy Department officials, who announced the \$94 million contract, said the computer will be used to simulate nuclear explosions so the government can test atomic bombs without actually blowing them up. Energy Secretary Hazel O'Leary said the new computer will be a "dramatic leapfrog" over currently available technology.

I guess eliminating an actual explosion, or "rapid disassembly" as the Air Force labels it, would reduce a lot of risks, wouldn't it? Hmmm.

I suspect we would soon be building weapons that would never work when the real trigger was actually squeezed.

I also suppose the next logical step for the government would be to use the new computer to test nuclear devices without actually building them. Just think how much safer the world would be. It could also be used to compare military forces of the world to determine which country wins a war without actually fighting the war. WoW, just think of all the lives that would save. Secretary O'Leary sure has my vote. uh-huh!

✶ Swiss address risks of holding referenda by Internet

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

Wed, 21 Aug 96 9:43:24 PDT

There have been recent proposals in Switzerland to hold their frequent national referendums via the Internet. The Swiss Federal Council has rejected a parliamentary request to pursue that approach, on the grounds that the computers and networks are too vulnerable to being sabotaged -- from almost any computer in the world. [Source: A Reuters item, 20 Aug 1996, noted by Dave Farber <farber@central.cis.upenn.edu. PGN Abstracting and Paraphrasing.] Perhaps they have been reading RISKS?

✶ Risks of remote-controlled fireplaces

Jeffrey Mattox <jeff@cher.heurikon.com>

20 Aug 1996 19:33:35 GMT

Friends of mine have a remote-controlled gas fireplace in their new home.

It allows them to turn the gas fire on and off from across the room.

Special logs are used for a gas fire, but the fireplace is designed to burn real logs, too.

One day, they came home to their empty house and found the fire was ON, but

the flue, which had to be manually controlled, was closed.

Since the flue

was closed, the smoke and flames from the real logs went into the house.

They were lucky -- just some localized fire and smoke damage -- but if the

fire had burned much longer, their home would be ashes.

The store says there have been similar incidents in the area.

Apparently,

some remote controlled toys operate on the same frequency.

Jeffrey Mattox -- jeff@heurikon.com

✶ Re: Escaping software upgrade hell

"Vladimir Z. Nuri" <vznuri@netcom.com>

Mon, 19 Aug 96 20:46:13 -0700

A summary of some additional points on this topic brought up by correspondents, identified by their initials, follows.

I mentioned several very useful capabilities that are not yet widespread or

going under common terminology. These are ranked below in order of

abstraction, complexity, cost, and degree of penetration. (With increasing

abstraction, greater cost and complexity, and fewer instances of

its
implementation.) Note that complexity and cost are issues that
relate to
both the design on one hand and use on the other.

1. Ease and seamlessness of switching between versions of code--
either
 forward during an upgrade or backward when incompatibilities
 or bugs arise.
2. "Shadowing" new code so that it is run and checked against
old code
 before put on live.
3. Computer control over code versions based on automated
reliability
 measurements-- software that actually controls when new
versions are
 added after reliability tests are passed or failed.

DCB mentions that old Multics and ARPA systems both "did real-
time updates
and rolled both forward and back between releases of
components", with a
lecture given on the subject once by Paul Stachour. This appears
to be an
instance of (1) and (3).

JWB complains of the cost and complexity of the above and
suggests
implementing any of these features may actually make software
more buggy in
the long run, and that trying to get to previously stable states
may
actually be more difficult.

SK says that (1) is apparent in disk controller hardware and
calls it "hot
swapping" of code.

HT says that "everything you describe [1-3] is regular practice
in telephony
hardware and software" with the caveat that "you have to build
systems from
the hardware up for this kind of [reliability]". He describes a

system by

Nortel: "essentially, yes, the system runs in shadow mode all the time, often shadowing a release with a duplicate of itself, but sometimes shadowing on a different release." "Duplicated systems are complex and hard to do right - they're also the bread-and-butter of telephony companies everywhere. Unfortunately, we don't blow our own horn as much as we should."

MS says that NASA is investigating on an ongoing basis modular hardware and software "hot swapping". Chorus Systems (France) is working with the European Space Agency and all components are "hot swappable".

AF says "You have some great ideas here. I agree that a fundamental shift in the way we think has merit. I have personally designed a software system that is designed with field upgrade in mind from the ground up". He mentions that in "closed loop system" however, it is far more difficult to directly compare to versions of software because their results are supposed to be divergent. I pointed out in a reply that software to measure whether this divergence is moving in the "correct direction" (via shadowing) would also tend to minimize upgrade glitches (in cases where the upgrade actually degrades performance).

SR writes that the real problem we are trying to solve is "incorrect software" and describes ways of improving software reliability before installing it. I am obviously in favor of doing that to the greatest extent

possible, but feel that there is a point of diminishing marginal returns in which exponential labor is spent in trying to remove the so-called "last bug". It is this view I was generally rejecting in the essay, by starting from the idea that even well-intentioned designers who have done all the reasonable testing possible cannot catch every bug. In fact I think the terms "correctness" and "bugfree" are highly misleading as a black-and-white view of a gray situation. Is there a "correct" instance of a complex piece of software anywhere in existence?

"Professionally, I feel that we need to ensure that software going out is as correct as possible" sounds as compelling to me as a politician stating, "I'm in favor of families." The major point of my essay was that even the best of engineers make mistakes that cannot be detected except in live use ("bugs happen"?), and paradoxically when we finally learn to accept that, instead of constantly pointing the finger at the engineer who made the mistake, we might begin to create systems that work in spite of them. I am increasingly skeptical of the claim applied to every bug, "the designers didn't test thoroughly enough"-- often it's too trivial an answer for too complex a situation. In other words, sometimes the best solution is building a better mousetrap, and other times it's figuring out how to make the existence of mice less catastrophic.

The case I was focusing on my essay was the situation where software *previously* works, and then *fails* to work in the same way

because of an upgrade. In this situation, *regardless* of designer fault, ideally the end-user would have enough control to fall back to prior base functionality gracefully. However, SR makes some very good points about methods of improving reliability prior to delivery, including considering the debugging and test code as an intrinsic part of the delivery, something I strongly advocate. In fact if clients increasingly began to ask prior to signing a contract, "what are you going to include in the system itself to catch errant behavior" instead of focusing on the resumes of the designers, we may all tend to be better off in the long run.

WC mentions Ericsson's Erlang language containing some of these ideas, designed to support high-availability systems like telephony:

<http://www.ericsson.se/cslab/erlang/>

In general, from responses I would conclude large Internet and cyberspace vendors may benefit significantly from studying techniques used in telephony to ensure continued and stable operation even during upgrades. Also, internet protocol designers may begin to look at telephony techniques for advancement in the bulging-at-the-seams internet network traffic. In fact the internet telephone software designers may eventually have to confront the same issues that telephone designers did many decades ago. Maybe future conference organizers in both areas might consider this aspect of promising cross-pollination.

In fact we appear to be in the beginning stages of the heralded "convergence" in which telephony and internetworking are in the early pangs of learning from each other prior to a merge into a unified cyberspace, with AOL and others realizing they are becoming more and more like utility services. With everyone's hard work, hopefully in the end we'll get the best of both worlds (reliability of telephony, flexibility of the internet) instead of the worst of both (flexibility of telephony, reliability of the internet)!

I am struck by the apparent lack of a single definitive reference on this critical subject. These techniques are spread out in aerospace, military, telephony, and other niche and proprietary areas and would benefit immensely from a systematic treatment by someone with a broad perspective. How about, "Creating Fault Tolerant Systems". It would be a great Yin to the Yang of the recent Risks book on the shelves by PGN. Any takers?

[Wouldn't it be great if someone wrote a journal that contained instances of software and hardware etc. that correctly handled a very difficult problem or catastrophic situation due to the ingenuity of the code? studying it might actually improve the world even more than RISKS. VZN]

✶ Re: London Train Crash ([RISKS-18.34](#))

Roger Hird <roger.hird@argonet.co.uk>
Wed, 21 Aug 96 10:09:06

I don't want to turn Risks Digest into a platform for political discussion on the privatisation of the British railway (BR) system, but there are background points worth making to put recent contributions in context.

The original item ([RISKS-18.32](#)) was based on a thin US newspaper report and the contributor commented that Risks Digest had a number of examples of rail incidents in London. This comment needs to be put into context. These incidents involved three separate systems: British Rail (BR), what we think of in the UK as "the railways", London Underground - London's subway system - and Docklands Light Railway, DLR, a new, small, overhead system serving redeveloped dock areas in East London whose teething problems with systems and software have attracted perhaps excessive attention. BR, the national railway system has not had all that many accidents/incidents in the London area. Of the ones explicitly identified with London there was one major one, some years ago now, the Clapham (sic - it was actually nowhere near Clapham) rail disaster due essentially to faulty wiring in a signal display. This was entirely relevant to Risks Digest. But I don't remember many/any other system related incidents on the BR network in or near London. There have been mechanical failure incidents, eg brake failures, with one death.

Alastair Scott's contribution (18.34) seems to be a fair summary of what is currently known about the train crash outside Watford. The comments on the

apparently greater safety of the modern rolling stock design are interesting.

There seems little doubt that, given the "black boxes", the survival of the drivers and the Health and Safety Executive enquiry (required by law in the case of any fatal rail crash, I believe) we should get reasonably reliable, and quick, conclusions about what went wrong.

But I thought Jim Reid's contribution less helpful. I'm a rail traveller and share his scepticism about the privatisation of Britain's railway system and the incredibly complex structure of franchises, leases, service companies and operating companies and leasing companies which it has spawned. But that is no reason to suspend ordinary principles of objectivity. There was no indication from anyone, and no serious allegation, that any factor in the latest crash resulted from or was exacerbated by the privatisation of the British Rail system or doubts or uncertainties about responsibilities or boundaries between the various companies involved. There were lots of transient problems of that sort as new structures were put into place (I remember, in 1994, days of frustrating buck passing between station operators and train operators as I simply tried to find out who was responsible for property lost on one particular train - I never did get back that CCTA digest on writing information system strategies) but they were transient. There are still some issues of concern but I hear of few serious doubts that safety operations are not co-ordinated. Jim Reid's points, except for one unreferenced anecdote about how very junior staff handled a small fire, are simply assertions and

expressions of opinion about what is happening and how the companies involved are behaving. The role of the Health and Safety Executive, which enquires into accidents, is clearly defined in statute.

Non UK readers may also get the impression from Jim Reid that the absence of ATP is a consequence of cost-paring decisions by private companies.

Clearly, decisions not to install ATP after privatisation are theirs, but they follow a long history of low investment in the state owned system.

Given the system they bought it is not unreasonable that the new owners should, in making safety related investments, go for the best value. If the statistic quoted by Alastair Scott is valid then new rolling stock might well be a better investment, both in safety terms and commercially, than ATP. Again, Jim Reid's comments on the investment strategies of the new privatised system are as yet predictions, not descriptions.

Finally, Jim Reid's comments on the ATP/rolling stock choice appear to query the concept that investment in risk avoidance can reasonably use cost benefit comparisons. Well, surely, that is what risk management is all about? We all do it individually, and qualitatively, in our decisions on safety in our homes and cars. Some people have formal risk management responsibilities: eg transport operators of all sorts, highway designers, power operators, air traffic control organisations. They have limited investment budgets and are constantly having to balance safety and commercial considerations in making their choices. They do this

quantitatively and formally and, in the public sector usually on the record
- and have done for decades. Assigning a value to lives potentially saved is part of this process. Risk elimination is ideal - but seldom affordable.

Roger Hird
uk

roger.hird@argonet.co.

<http://www.argonet.co.uk/users/roger.hird>

[There were many other messages on this subject, e.g., from Pete Mellor <pm@csr.city.ac.uk>, campbellp@logica.com (Peter Campbell Smith), Fieldhouse Dirk <Fieldhouse@logica.com>, Paul Smee <P.Smee@Bristol.ac.uk>, and Tim Sheen <eng407@abdn.ac.uk>.

Rather than try to pick out nuggets from each, I have selected the following note from Clive D.W. Feather. Perhaps those of you not included will add specific points if there are any remaining! PGN]

⚡ Re: London train crash

"Clive D.W. Feather" <Clive@demon.net>

Wed, 21 Aug 1996 10:52:22 +0100

There were two long items in RISKS about this crash. Both, I am afraid, present a distortion of the facts.

>What happened was that a train from Euston to Milton Keynes with about 400

>passengers on board was travelling North at about 60mph.

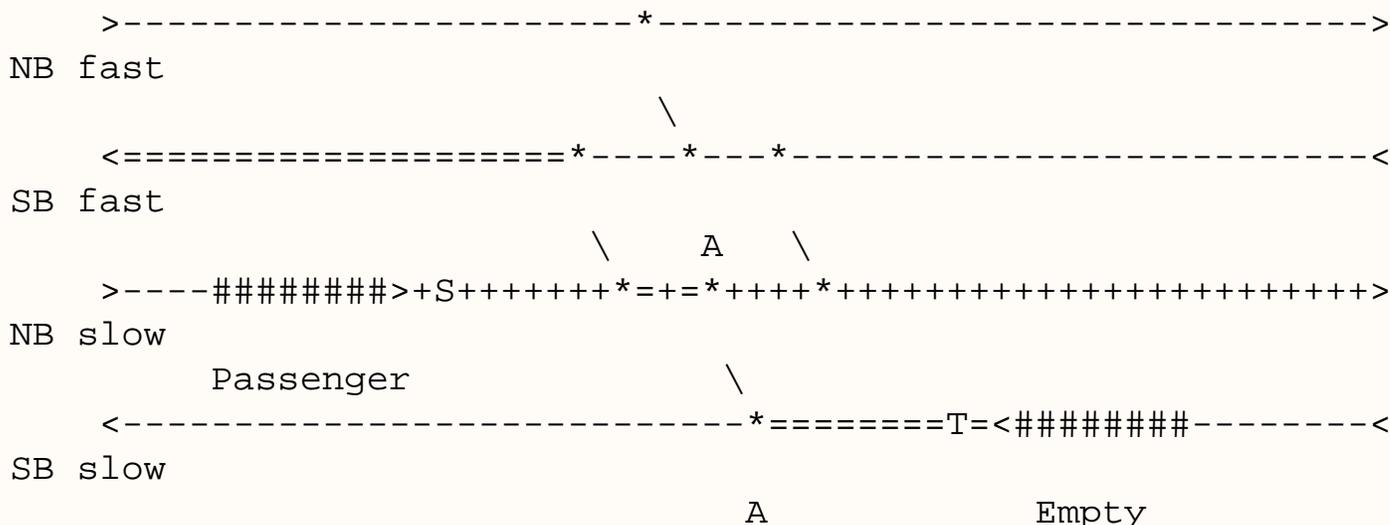
Another empty

>train, which should have been waiting at a red signal just outside Watford

>Junction, started moving slowly South and crossed over a set of points onto

>the North-bound fast line straight into the path of the fast train.

Given the layout of track here, *if* the signalling was operating correctly, then this cannot be a correct explanation. The actual layout is roughly:



The intended route of the passenger train is shown as +++++, and that of the empty one as =====.

The important point (sorry) is the pair of points labelled A. These always move together. If these points were set correctly for the passenger train and the empty train had passed signal T at Danger, then it would have run along the slow line and no accident would have occurred. But clearly AA (which is where the collision happened) was set for the empty train, and the passenger train passed signal S at Danger.

IF the signals were working correctly, then the facts tell us that the route was set for the empty train, and the passenger train passed a Danger signal. It is still possible that the empty also passed a Danger

signal, but we can't tell that from the evidence presented so far.

>"Black boxes" were recovered from both crashed trains, and showed that
>signalling and train systems were working properly just before the crash.

In which case the passenger train driver is primarily at fault.

>It was a huge stroke of luck that the collision involved new rolling stock:
>on some other lines carriages are 30 or 40 years old and are of an antique
>"slam-door" design which concertinas in the event of a crash.

Concertinaing, as a problem, was largely eliminated in the 1950s and 1960s. While it is true that these were slam door trains, that is not relevant to the issues.

> I have read
>that, of about 70 deaths on the United Kingdom railways in the past 10
>years, all but one have occurred in these older carriages.

Yes. But over half these numbers are due to a *single* event - the double collision near Clapham Junction. And there it was not concertinaing that caused the deaths, but the speed of the first collision followed by another train ploughing through the wreckage. And a good number of those left are due to people falling out of open doors. In other words, this statistic says nothing about the crashworthiness of these trains.

[Regarding Clapham, please recall an item in [RISKS-8.01](#) from Clive via Mark Brader, and another later one in [RISKS-8.85](#) from Jon Jacky. PGN]

>A number of risks have emerged from the recent crash. The first concerns
>Automatic Train Protection, ATP. This system is claimed to stop
>any train
>which passes a red signal. It is not used on the British
>railway network,
>though it is deployed on other European railways. [Apologies to any
>trainspotters for any simplification I've made.] The UK railway
>companies
>say that ATP is too expensive - it costs too much for each life
>it saves,
>though how they work that out is beyond me. (Another risk?)

This is actually fairly simple to determine. The costs of
complete ATP
installation are known. A record is kept of all accidents and
their
causes, and so it is simple to determine how many lives and
injuries
would not have happened in (say) the last 20 years if ATP had
been
installed at each place. Divide.

> They claim that
>the money required for ATP would be better spent on other
>safety measures
>like modern, stronger passenger carriages. So, rather than
>prevent trains
>crashing into each other, they think the best strategy is to
>let them crash,
>but make the rolling stock safer. (Yet another risk?)

Not all accidents would be prevented by ATP - apart from
anything else,
ATP failure is an extra possible *cause* of accidents. The
calculation
is more like this (numbers are illustrative, not exact):

ATP installation costs 400 million pounds and saves 10 lives.
Anticlimber installation costs 30 million pounds and saves
15 lives.

Which is the better spend ? Especially given that the government has reneged on its promise to fund ATP.

>The next risk is the absurd way in which Britain's railways are now run
>after privatisation.

Unfortunately all too true.

>For the leasing companies, repainting old trains is more cost effective than buying new ones which presumably have better safety features.

>For the operating companies, the cost of leasing is one of the few costs

>they can control. [They can also work their drivers harder, but that will be

>another safety risk.] Thus, they prefer to run old, less safe, trains

>because they are cheaper to lease than new ones.

Not necessarily the case. In particular, the leasing prices were set so

that the cost of old trains was the same as that of new ones; it is

claimed that this will encourage investment in new trains, as operators

will prefer them.

Clive D.W. Feather, Associate Director, Demon Internet Limited

⚡ Re: London train crash

<mpoole@uhea904.gb.ec.ps.net>

Wed, 21 Aug 1996 12:27:33 +0100 (BST)

There is one piece of information which does not seem to have made

it into general circulation regarding the crash.

The northbound train (with the passengers) was the 17:04 which left on time.

The preceding northbound train (16:54) was delayed by over 6 minutes which

meant the southbound (empty) train would have been delayed by at least that

in crossing over onto the other line.

Martin Poole, Perot Systems Europe mpoole@uhe904.gb.ec.ps.net

✶ "Authentication Systems for Secure Networks" by Oppliger

"Rob Slade" <roberts@mukluk.hq.decus.ca>

Tue, 20 Aug 1996 10:24:30 EST

BKAUSFSN.RVW 960608

"Authentication Systems for Secure Networks", Rolf Oppliger, 1996, 0-89006-510-

1

%A Rolf Oppliger

%C 685 Canton St., Norwood, MA 02062

%D 1996

%G 0-89006-510-1

%I Artech House/Horizon

%O 617-769-9750 800-225-9977 fax: +1-617-769-6334 artech@world.std.com

%P 186

%T "Authentication Systems for Secure Networks"

Given the relative scarcity of knowledge about data and communications

security, it seems rather odd to find a security book which comes right out,

first thing, and say that it is not intended to be tutorial.

However,

Oppliger does not spend much time on the basics. (There is a general

introduction to security terminology and techniques, but only one chapter.)

The emphasis of the book is on the explanation, review, and comparison of various systems for ensuring the security of communications within a network over which the security of physical links may be in doubt.

The systems covered include Kerberos, NetSP (Network Security Program), SPX (Sphinx), TESS (The Exponential Security System), SESAME (Secure European System for Applications in a Multivendor Environment), and OSF DCE (Open Software Foundation's Distributed Computing Environment). Kerberos get the most space, probably since most of the rest are variously expansions or refinements of the basic Kerberos concepts. The examinations are detailed, although not to the level necessary for implementation, and the overview looks into individual strengths and weaknesses. A final chapter does a side by side comparison of the systems in terms of functions, cryptographic techniques, standardization, availability, and exportability.

copyright Robert M. Slade, 1996 BKAUSFSN.RVW 960608

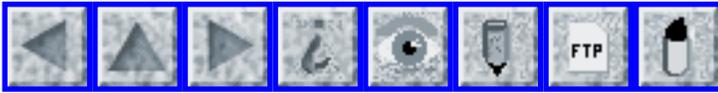
roberts@decus.ca

rslade@vcn.bc.ca

rslade@vanisl.decus.ca

Author "Robert Slade's Guide to Computer Viruses" 0-387-94663-2
(800-SPRINGER)

[For those of you who have not read it, please note the RISKS policy on the redistribution of copyrighted materials submitted to RISKS: see risks.info or risksinfo.html, cited below. 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 18: Issue 37

Thursday 22 August 1996

Contents

- [Karpov versus the world via Internet](#)
[PGN](#)
- [SSN problem hits a Congressman](#)
[Stanton McCandlish](#)
- [Easy answer on porno?](#)
[Tim Barmann via Dave Farber and Stanton McCandlish](#)
- [Rich folks embrace digital privacy and anonymous markets](#)
[Peter Wayner](#)
- [Re: Internet Explorer security problem](#)
[Thomas Reardon](#)
- [Inability to tinker not confined to hardware](#)
[Scott Alastair](#)
- [Re: Computer testing of nuclear weapons](#)
[Robert Herndon](#)
[Mark Stalzer](#)
[Barry Jaspán](#)
[Frank C. Ferguson](#)
- [Measuring software time to repair](#)
[Stu Savory](#)
- [Long-running systems](#)
[Martyn Thomas](#)

● [Call for Participation: SEI Conference on Risk Management](#)

[Carol Biesecker](#)

● [Info on RISKS \(comp.risks\)](#)

✶ Karpov versus the world via Internet

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

Thu, 22 Aug 96 14:46:39 PDT

An unusual kind of Internet chess game will be held next week in Finland, sponsored by Telecom Finland. Anatoly Karpov will be pitted against the consensus of a collection of on-line participants, estimated to be around 50,000 in number, where after each of Karpov's moves the wannabes get 10 minutes of real time to think, and a Telecom computer will pick the most popular move. Check out <http://www.tele.fi/karpov> for details.

What are the risks?

1. What if 100,000 opponents show up and overwhelm the website?
2. Will a dumbed-down consensus result? Can a few master-level players have any impact over a horde of average players?
3. How can any coherent strategy emerge from such a consensus strategy?
4. Could the resulting somewhat randomized strategy actually be more effective than a more coherent strategy? (Garry Kasparov had an interesting time figuring out IBM's Deep Blue strategy, and beat it with a less coherent approach than he might normally have taken.)

See [RISKS-17.79.](#))

5. Could Kasparov hack his way into tele.fi and reprogram the software

so that only HIS move was tabulated? Certainly the organizers could

do that, but it would spoil the fun.

6. Could Karpov use a Finnish anonymizer and then, if he lost, repudiate

the results by claiming it was really Kasparov who was playing?

🔥 SSN problem hits a Congressman

Stanton McCandlish <mech@eff.org>

Thu, 22 Aug 1996 11:35:54 -0700 (PDT)

I received a press call this morning asking about Social Security Numbers and database privacy in general, from a journalist covering a story that should have happened years ago.

A US Congressman running for Governor of New Hampshire was found to have two SSNs by local journalists, who ran a story on it. (It's illegal to obtain 2 SSNs in most circumstances, so one supposes this seemed newsworthy).

After the story ran, it turned out that the other SSN belonged to a teenager, and that the legislator had been assigned the number (presumably in some marketing or DMV or other error-prone database) by mistake.

Despite the situation not being the legislator's fault, his chances for election to the Governor post have been damaged by the bad reportage,

possibly ruined.

At this point, I don't have the name of the legislator, nor of the paper and journalist(s) who reported on this.

Many obvious RISKS that have come up before plenty of times in RISKS:

- 1) SSNs are not a good system - they are neither truly unique identifiers, nor is the system even close to immune from errors or fraud.
- 2) Even "minor" data entry errors in databases of personally identifiable information can ruin careers and otherwise wreck people's lives, but there's not really any easy way to detect these errors or to fix them until they cause a personal, or sometimes far broader, catastrophe.
- 3) There is no real accountability, even aside from privacy issues. State laws are scattershot and disparate, affording little privacy protection and even less recourse when negligence wreaks havoc. They are so different from state to state that even an industry-generated code of conduct doesn't arise. At the federal level, it's even worse.
- 4) Reporting on technical topics, like information held in databases, can be rapidly screwed up if the reporters do not take care to get the facts, but simply report what seems obvious on the surface. (C.f. Time's "Cyberporn" cover story for another infamous example.)
- 5) Blind trust in technology - "the computer is always right" - can lead to quite harmful mistakes. It appears that the reporters who jumped on this story accepted it as a given that the legislator had obtained

two SSNs
for some nefarious purpose, and missed the far more likely
possibility:
data entry error by a third party.

[This is based on what I've been told about these events and the
reportage of them. I have yet to see the original articles,
though I
expect to get them shortly. So, some of this criticism is best
considered
hypothetical, until I do have the articles. I cannot, of
course, be
certain of the accuracy of the characterization by one
journalist of
another and his/her work.]

As for why I say this should have happened a long time ago, this
is the
first time I've heard of something like this happening to a
policymaker.
Hopefully the nature of the problem will sink in and we'll see
some action
to establish accountability and privacy-protection
requirements. At very
least, the dismal failure of the SSN may become more apparent to
Congress,
who have simply not appeared to grasp the nature of the problems
to date.
The new crypto-awareness on the Hill could use a strong booster
shot of
general privacy awareness.

Stanton McCandlish Electronic Frontier Foundation mech@eff.org
"<http://www.eff.org/~mech/>"

[This saga is quite skimpy, but is the best available at the
moment. I hope someone can fill in the details for us. PGN]

✶ Easy answer on porno? (Tim Barmann via Dave Farber)

Stanton McCandlish <mech@eff.org>
Thu, 22 Aug 1996 12:16:18 -0700 (PDT)

[Via Dave Farber <farber@central.cis.upenn.edu>]

>From: Timothy Barmann <tim@cybertalk.com>
>Subject: Warning from Family Circle Magazine

Got this amusing/disturbing press release from *Family Circle Magazine*,
apparently to promote an upcoming article. It reads:

>CERTAIN COMPUTER FILE LETTERS INDICATE PORNOGRAPHY: POLICE CHIEF
>

>New York -- Parents can safeguard their children against
pornography on
>the internet by watching for files stored on a computer's hard
drive or
>diskettes that end in the letters -PCX, -GIF, -GL, TIF, or -
JPG, according
>to the current (September 17) issue of Family Circle. "Those
are the
>graphic image files that may be pornographic, and parents
should know what
>they illustrate," says Police Chief Alfred Olsen, who monitors
online
>predators in Pennsylvania.

I'm surprise that TXT was left out, which of course is the
format used to
distribute sexually explicit words as well.

Timothy Barmann, *Providence Journal-Bulletin* tim@cybertalk.com
401-277-7369 <http://www.ids.net/~tim/> [http://www.ids.net/
cybertalk/](http://www.ids.net/cybertalk/)

⚡ Rich folks embrace digital privacy and anonymous markets

Peter Wayner <pcw@access.digex.net>

Tue, 20 Aug 1996 21:18:10 -0400

Two items from the recent news:

1) The August 7th edition of the WSJ has a front page story on the divorce of cellular phone king, Craig McCaw. Here's the salient phrase, "... Mr. McCaw says in an interview via a wire-line phone to which he entrusts all sensitive conversations because he is leery of eavesdropping on his cellular calls." Given that the call was at least partly on the record, I wonder how he handles his truly sensitive calls.

2) The August 20th edition of the NYT describes the effects of the recent settlement between NASDAQ and the SEC. The NASDAQ marketplace is essentially a computer network that links a group of dealers who use the system to make announcements like "I want to buy Microsoft for 92 dollars/share." A brokerage firm will often make a profit on the difference and not pass it on to their customers. If someone breaks the spread, all of the brokers suffer but the customers generally gain a small advantage. The SEC now has audio tapes of some dealers using collusion and social pressure to keep the spreads up between the price the shares are offered to buy and sell.

There is also another market ran by Reuters known as "Instinet" and it is anonymous. No one knows who is offering to buy and sell shares. If someone breaks from the pack and starts offering slightly more money for a particular issue, there is no easy way for the dealers to retaliate. It's

all anonymous. The article suggests that prices are often fairer for the people who use Instinet. Of course it is only open to big folks like institutional investors. Presumably it is not truly anonymous and the SEC could unwind the trades if it wanted to investigate, say, insider trading.

✉ Re: Internet Explorer security problem (Felten, [RISKS-18.36](#))

Thomas Reardon <thomasre@MICROSOFT.com>

Thu, 22 Aug 1996 15:49:33 -0700

>We have discovered a security flaw in the current version (3.0) of >Microsoft's Internet Explorer browser running under Windows 95. An >attacker could exploit the flaw to run any DOS command on the machine >of an Explorer user who visits the attacker's page.

We now post the virus warning dialog on local files (file: urls). We have always posted it on remote files (http: urls). Note that the root of the problem is not Java or the browser, but in macro-enabled applications. IE3 has a mechanism to warn users about safety of documents when used with common macro-enabled applications. We are have updated Microsoft Word such that by default it will not run macros embedded in documents.

-Thomas

✶ Inability to tinker not confined to hardware

"Scott Alastair (Exchange)" <ScottA@logica.com>

Wed, 21 Aug 1996 15:09:33 +0100

People can't tinker with software either these days ... for example, there is no programming language supplied with Windows 95.

>From this, a RISK is that a program of any degree of triviality may be seen by a lay person as miraculous. I wrote a Word for Windows macro to generate chess board positions out of sheer necessity - I needed pictures for a magazine article I was writing and no software I had could generate them easily. I then realised that my macro might be useful to other people. So I uploaded it to an archive site - and the response was phenomenal, with emails coming in by the dozen praising what I have done. Yet the macro is made up of about fifty lines of code, there are no devious tricks and the algorithm used to generate the chess board from user input is relatively simple. I am a software engineer; if I was incapable of writing such a macro I would wonder whether I was fit to be called a software engineer.

Who was it who wrote that "any sufficiently advanced technology is indistinguishable from magic"? They are right, and they are becoming more than right.

Alastair Scott <scotta@logica.com>

✦ Re: Computer testing of nuclear weapons (Ferguson, [RISKS-18.36](#))

Robert Herndon <robert.herndon@Central.Sun.COM>

Wed, 21 Aug 1996 18:12:24 -0600

Frank Ferguson <ferguson@dmapub.dma.org> notes in [RISKS DIGEST 18.36](#) that

the U.S. Department Of Energy has signed a US\$94M deal with IBM to develop a new supercomputer designed specifically to simulate nuclear explosions.

Frank's conclusions, however, don't follow.

The U.S. DOE is almost certainly the worlds' largest consumer of high-speed computers used for simulation, and has in fact been instrumental in the funding and development of these computers. Richard Rhodes' books on the development and construction of the first A and H bombs makes this abundantly clear, as do many other books on the subject, and others on other subjects (e.g., Richard Feynman's book that mentions his activities during WWII). Many U.S. DOE atomic labs already have large supercomputer centers devoted to simulation.

While the purpose of the computers is to simulate nuclear events, their intended purpose is not generally to eliminate all nuclear tests. The computer codes are worth discussion. They are, as a former chairman of CDC noted in a speech many years ago, the human race's best understanding of nuclear events. As a result, these codes are highly classified. A great many complex, coupled, and inter-related phenomena occur during an

explosion. Among them are radiative, particle, and shock phenomena. The need for models of these phenomena was probably first determined by Hans Bethe, several years before the first A bomb explosion, and it was also he who first developed the idea of Monte Carlo (probabalistic) simulation.

While the physics of each individual aspect of a detonation is well understood, their coupling is very complex. E.g., radiative opacity is determined in part by temperature, which is affected by radiative and particle absorption. Many of the constants affecting these phenomena and their couplings cannot be determined accurately by a priori computation, and must be measured or approximated.

As a result, the computer models are the only way, other than actually detonating a device, of accurately estimating the yield and efficiency of a new design. In complementary fashion, the only way of reliably improving the accuracy of the simulation codes is fashioning devices and measurement equipment and testing them. This is in fact done.

Indeed, I have been given to understand by several knowledgeable people that the purpose of nuclear tests is most often to verify improvements to the computer models. It is a deep-rooted need of humans to understand the universe. The codes modeling the detonation of nuclear devices would appear to be monuments to this (cold-war fear, too, I imagine). The rapid development of the neutron bomb (er, "enhanced radiation device") would appear to be a testament to the reliability and accuracy of

these codes.

Certainly, the current efficiency of nuclear devices is such that extinction of the human race can be safely assured, if such a goal is considered desirable. It becomes perhaps questionable, then, what additional sophistication in the simulation and design of nuclear devices is intended to accomplish, beyond satisfying this curiosity.

The risk is slight that the U.S. will design, build, and deploy nuclear devices that fail to work due to failures of the computer models. Fear that physical/computer models might not be reliable was definitely responsible for tests of cruder-than-necessary bombs (e.g., the USSR's first A and H bombs, and several early U.S. devices (see Rhodes' books)).

The risk seems many orders of magnitude greater that, due to test bans, the U.S. will spend large sums of money simulating and designing nuclear devices that it cannot test, manufacture, or deploy. In the absence of test ban treaties, the risk is that the U.S. will detonate additional devices to verify the more complex models that the faster computers will allow (highly probable).

Robert Herndon

✉ Re: Computer testing of nuclear weapons (Ferguson, [RISKS-18.36](#))

Mark Stalzer <stalzer@macaw.hrl.hac.com>

Thu, 22 Aug 1996 13:53:13 -0700

In [RISKS-18.36](#) Frank C. Ferguson <ferguson@dmaphub.dma.org> takes some issue with the idea of relying on computers to design nuclear weapons.

He writes in part:

>I guess eliminating an actual explosion, or "rapid disassembly" as the Air

>Force labels it, would reduce a lot of risks, wouldn't it?

Hmmmm.

>

>I suspect we would soon be building weapons that would never work when the

>real trigger was actually squeezed.

Computers are useful for many simulations related to nuclear weapons

other than designing clever little devices that rapidly disassemble in

spectacular ways. A few examples are:

a. predicting the destructiveness of a particular device with known

characteristics (determined by testing) when used in a particular area.

b. predicting the fallout in various geographic areas and weather conditions.

c. finding out what happens if a device is accidentally smashed, eg.

is unintentionally dropped from a plane (this has happened many times!),

does it blow up or is the bomb stuff contained?

d. performing fusion energy experiments prior to building the apparatus.

e. refining existing designs and exploring completely new concepts.

Many tasks involve taking known weapons and exploring their behavior in

situations where real testing is impossible. Even if the US stopped all

weapons design, there would have to be a lot of simulation just to explore the capabilities, limitations, and safety related issues of the current stockpile.

Some WWW references to IBM's and Intel's new machines and their applications are:

<http://www.austin.ibm.com/Cover/Announce.960726/doespress.html>

<http://www.ssd.intel.com:80/tflop.html>

It should be noted that weapons work is just a part of what's planned for these next generation supercomputers.

Mark Stalzer, mas@acm.org

[Other comments on this topic also received from
"Christopher Duro" <cduro@softkey.com>
nelson@berlioz.nsc.com (Taed Nelson)
Jerry Bakin <bakin@haas.berkeley.edu>.
PGN]

⚡ Re: Computer testing of nuclear weapons (Ferguson, [RISKS-18.36](#))

"Barry Jaspán" <bjaspan@MIT.EDU>
Wed, 21 Aug 1996 15:06:07 -0400

I recently pointed out how the plot of the movie `_The Running Man_` was the same as a something suggested here in RISKS. So I cannot avoid mentioning:

```
>> to use the new computer ... to determine which country wins a
war without
>> actually fighting the war.
```

The original Star Trek episode "A Taste of Armageddon" was based

on exactly
this premise. There is nothing new under the sun...

Barry

[Noted in greater detail by "Jonathan I. Kamens" <jik@cam.ov.com>. PGN]

✂ Re: Computer testing of nuclear weapons ([RISKS-18.36](#))

"Frank C. Ferguson" <ferguson@dmapub.dma.org>
Thu, 22 Aug 1996 14:56:43 -0400 (EDT)

[In response to Jonathan Kamens noting Star Trek was 30 years ago.]

Actually I think the ancient Chinese were the first. They simply assembled opposing armies on opposite hilltops while the intermediaries met in the valley. They decided which army was most likely to win and then they all returned home.

Frank Ferguson

✂ Re: Measuring software time to repair

Stu Savory <savory.pad@sni.de>
Wed, 21 Aug 1996 10:03:08 +0200

Further to David Holland's comments...

Here (at Siemens Nixdorf Informationssysteme) incoming bug-reports are classified 1 through 4 in severity level as perceived by the

user.

They are also classified according the department responsible for the code (1 through N). For each of these 4*N classes we have the historical statistical distributions of (inter alia) bug fix times and bug densities as well as improvement trends (and some other correlations ;-)

Inasmuch as one is able to predict the future statistically from the past, we are able to say something like "There is a (50/90/99%) chance that this bug will be fixed within time T".

I don't think you can do much better than this in the long run. I tried training a neural net last year, but the prediction accuracy doesn't seem to be much better (usual statistical test).

Dr. Stuart Savory Dept. of Quality & Customer Satisfaction.

⚡ Long-running systems

Martyn Thomas <mct@praxis.co.uk>
Wed, 21 Aug 1996 10:56:22 +0100 (BST)

We have had a request from a client to rerun the training course on how to start a system we delivered to them. It hasn't stopped for 18 months and they have lost confidence that they can restart it if they need to do so.

So, it isn't only systems that get patched and warm-booted that lose the ability to be cold-booted.

Is this a risk arising from delivering high-quality software?

Martyn Thomas, Praxis plc, 20 Manvers Street, Bath BA1 1PX UK.
Tel: +44-1225-444700. Email: mct@praxis.co.uk Fax: +44-
1225-465205

✦ Call for Participation: SEI Conference on Risk Management

Carol Biesecker <cb@SEI.CMU.EDU>

21 Aug 1996 20:40:10 GMT

Call for Participation - Software Engineering Institute (SEI)
Conference on Risk Management: Managing Uncertainty in a
Changing World

Hotel Cavalier, Virginia Beach, Virginia, April 7-9, 1997

Keywords: acquisition, programs, projects, systems, and software

Note: this is an abbreviated call for participation [and
excerpted for RISKS].

For complete information, please see

<http://www.sei.cmu.edu/products/risk97>

The SEI Conference on Risk Management will provide a forum that
brings

together representatives of government, industry, and academic
managers.

Practitioners, change agents, and researchers who use and
explore risk

management, system development and acquisition will detail the
latest

methods, tools, and techniques in the field.

This conference will provide a unique opportunity to

- * Increase your awareness
- * Advance your knowledge and skills
- * Exchange ideas and experiences with experts
- * Learn the latest methods, tools, and techniques and best
practices

of acquisition, systems development, and risk management

* Find out what's new, what's going on, and what could be useful for you

September 19, 1996: deadline for submitting papers and workshop proposals

For more information about the conference, contact--

SEI Customer Relations

Software Engineering Institute

Carnegie Mellon University

Pittsburgh, PA 15213-3890

Phone 412 / 268-5800

FAX 412 / 268-5758

Email customer-relations@sei.cmu.edu

World Wide Web <http://www.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 18: Issue 38

Monday 26 August 1996

Contents

- [More on the American Airlines Cali crash](#)
[PGN](#)
- [DarkStar UAV crash from software change - cost, \\$39M](#)
[David Wheeler](#)
- [Electric meter halts mail/news server](#)
[Kolja Waschk](#)
- [Denial of service attack brings down Netcom listservers](#)
[Sidney Markowitz](#)
- [DNS failure \[from Matthew Dillon\]](#)
[Steven Weller](#)
- [Re: SSN problem hits a Congressman](#)
[Craig Neth](#)
- [Microsoft's warning](#)
[Mike Walsh](#)
- [Microsoft's patch](#)
[Ed Felten](#)
- [Why Java, Bash, Explorer, and other bugs keep hurting us](#)
[Fred Cohen](#)
- [Too much integration](#)
[Nick Brown](#)

- [Re: Computer testing of nuclear weapons](#)
[Frank C. Ferguson](#)
[Jake Donham](#)
[Mike McKinlay](#)
 - [Year 2000 Bites the Budget](#)
[Frank Christensen](#)
 - [Re: London train crash](#)
[Clive D.W. Feather](#)
 - [Re: "Inability to tinker not confined..."](#)
[Tom Zmudzinski](#)
 - [Once more Murphy's Law](#)
[Jim Horning](#)
 - [Dependable Computing for Critical Applications, Final Call for Papers](#)
[Catherine A. Meadows](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✈ **More on the American Airlines Cali crash**

"Peter G. Neumann" <neumann@csl.sri.com>
Fri, 23 Aug 1996 15:13:43 PDT

"David L. Oppenheimer" <davidol@CS.Princeton.EDU> and jeisner@unagi.cis.upenn.edu (Jason Eisner) sent me the identical item, one from the AP and the other from *The New York Times*, 23 Aug 1996, entitled

Wrong Computer Command Led to Colombia Crash of American Airlines Boeing 757

American Airlines has noted that the pilots of the December 1995 crash of Flight 965 were lost at the time, and attributed the crash to the captain entering a computer command that steered the plane in the opposite direction. Unfortunately, the one-letter code for Cali on the flight chart they were using was the same as the one-letter for Bogota, and

caused the
plane to fly into a mountain, killing 159 of the 163 people
aboard. Pilots
have been alerted as to the discrepancies. (Most airline
computers use
different codes for the two cities.)

✈ DarkStar UAV crash from software change - cost, \$39M

David Wheeler <wheeler@ida.org>

Fri, 23 Aug 1996 12:33:47 -0400

An uncoordinated software change cost \$39 million, as reported in
"Inside the Air Force", July 5, 1996, page 10:

"Lockheed Martin and Boeing completed negotiations last week on
how to
split the team's share of the \$39 million cost of replacing the
high-altitude
unmanned aerial vehicle [UAV] which crashed in April near
Edwards AFB, CA.

The partners will split equally what could be a \$6 million to
\$12 million
bill from the Pentagon for the destroyed DarkStar, the same
proportion
by which it divides the workshare of building the UAVs.

The first flying DarkStar crashed shortly after take off from
Edwards
on April 22, resulting in the total loss of the air vehicle, the
only
flight test asset available at the time.

Although finger pointing has been assiduously avoided by both
companies,
industry and Air Force sources said the crash was the result of
Boeing
having adjusted software controlling flight on the UAV without
commensurate
changes being made in the system by Lockheed Martin's Skunk
Works division.

'The left hand didn't know what the right hand was doing,' a

source said.

However, the problem has been addressed and the program should be back on track shortly, pending the approval by the companies' lawyers of the terms of splitting the cost for the crash.

A May 16 letter to Rep. John Murtha (D-PA), the ranking minority member of the House Appropriations national security subcommittee, from Defense Airbourne Reconnaissance Office chief Maj. Gen. Kenneth Israel tagged the cost of rapidly configuring another DarkStar UAV for flight and making up lost time in the program at \$39 million."

[reprinted with permission from "Inside Washington Publishers - Defense

Group". Permission Point of Contact: Richard Lardner, U.S. (703) 416-8530]

Related URLs include "<http://www.boeing.com/dsg.darkstar.html>" and "<http://www.afa.org/magazine/6-6nn96.html>".

--- David A. Wheeler dwheeler@ida.org

⚡ Electric meter halts mail/news server

Kolja Waschke <kawk@yo.com>

24 Aug 96 21:24:23 +0200

I run a mail + news server at my home, serving only a few people but to these the ability to receive and send e-mail is quite important.

Recently I had to leave home for a couple of weeks. I spent a lot of time before to make the system quite fail safe, especially so

it could handle some tasks that I otherwise do manually. While I was away, it worked more reliably than at any time before. Until one day. It was not accessible anymore. I could not even call into a backup PC which was there just to provide at least the ability to reboot the server system.

Why ? The wheel in the electric meter (a 35 or more years old electromechanical device) used for counting the power consumed by the system, somehow stopped rotating. I assume due to a problem in the bearing it was not able to restart rotating after a simple power blackout (it restarted after giving it a slap, manually). Well, this meter was designed to limit the current to whatever it could count. Thus, no rotation, no current.

I understood that I'm responsible for the reliable operation of the PC hardware and software, and I can rely on the power supplied by my PSC. But I forgot there was one important device between their output and my system.

Kolja Waschk (kawk@yo.com, NIC-handle KW84) Tel +49-40-8891-3034 BBS/Fax -3035
<http://hp00.rz.tu-harburg.de/users/sekw0206> "Yo.COM news & mail service ..."

⚡ Denial of service attack brings down Netcom listservers

Sidney Markowitz <sidney@research.apple.com>
Fri, 23 Aug 1996 06:01:39 -0700

A mailing list I subscribe to started sending an endless loop of bounce

messages and another subscriber forwarded the following as explanation. I have not verified the authenticity of the message with Netcom, but I have no reason to doubt it. There are two denial of service attacks here: A person was email bombed by someone who subscribed him to many mailing lists, and then that person retaliated by bringing down the mailing lists. Once again we see an old problem that could have been prevented had the system administrators simply configured known security measures before their system was hacked.

[begin quoted message]

Newsgroups: netcom.announce
From: nc0022@netcom.com (Margaret)
Subject: Temporary hiatus of mailing lists
Reply-To: support@netcom.com
Organization: NETCOM On-line Communication Services (408 261-4700 guest)
Date: Thu, 22 Aug 1996 03:42:16 GMT
Approved: netmail@netcom.com

Outgoing mail from Netcom mailing lists is temporarily being delayed due to a mail looping problem, starting at 5:30 PM PDT today.

The problem was caused by a user at another site; someone subscribed him to many Netcom mailing lists, and he responded by creating an infinite loop of "bounce messages" to all the list subscribers. List mail is being queued until we can filter out these error messages.

Netcom is currently in the process of upgrading majordomo, and we hope to implement improved security for all our lists. In the interim, we

strongly recommend that listowners set their lists to "closed";
this
protects against all mass-subscription attacks.

Delivery of list mail should resume later this evening. Thank
you for
your patience.

[end quoted message]

-- Sidney Markowitz <sidney@research.apple.com>
Apple Research Laboratories, Apple Computer, Inc.

✶ DNS failure [from Matthew Dillon]

Steven Weller <stevenw@best.com>
Sat, 24 Aug 1996 08:53:31 -0700

The following describes DNS meltdown at my ISP the other day:
all DNS
services were unavailable, despite multiple servers being
online. Lack of
DNS assured that other working services were unavailable to
everyone who
didn't have IP addresses written down.

Here is a technical explanation of the DNS failure, for
those of you
interested.

First, a synopsis of how DNS works... every site on the net
serves their
own DNS records. Some sites serve other people's DNS
records. For
example, BEST serves the DNS records for best.com, best.net,
and most
of our customer's custom domains. No site serves more than
a small
fraction of the DNS records on the internet from their own
database.

The way DNS works is that when a domain name needs to be resolved, our

DNS server (anyone's DNS server) first goes to the NIC to ask where to

go to resolve the domain name. The NIC itself cannot resolve domains,

it can only tell our DNS server where to go to resolve a domain.

Our DNS server then goes to the specified remote site to resolve the

domain name belonging to that site. The remote site replies with the

answer which our DNS server (a) caches for future reference, and

(b) returns to the original requester.

The caching is important, because otherwise a DNS server would have to

re-query the remote DNS server every time someone wanted to resolve a

domain. DNS records propagate through caches. It is simply not possible

to run a DNS system with caching turned off, it would create an impossible

load on the internet.

Around 4:00 a.m. yesterday, some unknown site's cache got corrupted.

The corruption propagated to many (hundreds) of other sites on the internet

and eventually propagated to us. This corruption hit a bug in the DNS

server program that wound up corrupting the program, causing DNS to

lose major records.

Restarting the server in this case does not solve the problem because,

due to the caching on remote sites, the corrupted record repropagates

almost instantly. BEST was hit by this problem very hard

due to the

large number of custom domains we serve... so many DNS requests come into

BEST and are made by BEST that our servers would hit the corruption out on the internet within 10 seconds of starting up.

Worse, this particular corruption tended to destroy the root records

(stored in memory), called SOA records, for the domains served locally.

This destroyed the mail system causing mail messages to bounce rather than

to simply be delayed, because the DNS server was saying 'site X does

not exist' rather than timing out. It's worst possible corruption that

can occur in a DNS system.

--

It turns out that the last two BIND releases contain a bug that,

when a corrupted record of the type that started propagating at 4:00 a.m.

is received, results in the destruction of other ****unassociated****

records stored in memory.

The particular release of BIND that we were using had been running

perfectly for several **months** before this incident. It was not something

recently installed.

There are two fixes to the problem: (1) One can lock out those sites

where the corrupted records come from, and (2) One can revert to an older

release. (1) is not a good solution because, due to the nature of DNS,

corruption can propagate to many sites and it would be impossible to keep

up to date and lock all of them out. We wound up taking action #(2)

and reverting to an older release of bind which, fortunately, did not

have the bug that caused the problem. We had to revert to BIND 4.9.3.

Unfortunately, we did not think to do this for many hours because we were

all convinced that the problem was external in nature and just didn't

think to try a reversion. In hind sight, that is the first thing we

should have tried since we had the friggin binary for the older version

sitting in our source tree.

As far as DNS goes... the DNS we run is not 'bsd' or 'sgi' .. it's the

official world-wide BIND distribution run by Paul Vixie. It is really

not appropriate to run the older versions shipped with most operating

systems due to massive, massive security holes. The corruption problem

was unavoidable. What *was* avoidable was the long period of time that

elapsed before the problem got fixed, which I take full responsibility for.

We spent most of that time trying to track down where the corruption was

coming from... a near impossible task. Around 6:00 p.m. scuttlebutt

started propagating regarding a possible bug in the last two BIND releases

at which point we instantly reverted to an earlier version, which fixed

the problem, then started banging our heads against the wall for not trying

it earlier.

Matthew Dillon Engineering, BEST Internet Communications, Inc.

<dillon@best.net>

✉ Re: SSN problem hits a Congressman (McCandlish, [RISKS-18.37](#))

Craig Neth <neth@zk3.dec.com>
Mon, 26 Aug 1996 10:42:24 -0400

Early last week, the Nashua, NH *Telegraph* ran a front page story about U.S. Congress Bill Zeliff, who is current running for Governor of NH. The story asserted that the paper had discovered that the Honorable Mr. Zeliff was registered for two SS numbers. The excerpts I have seen from the article indicated that the reporters from the newspaper had contacted two 'out of state' database firms that collect information from various sources and make it available to various parties. The data showed two SSN numbers for Mr. Zeliff, one that was clearly his and one that looked to have been created rather more recently.

The next day, the headline was something to the effect that the two numbers might in fact be a database error, and included quotes from the database firms saying that errors in these databases were common, and that they are not responsible for errors - the errors are in the submitting systems, not theirs. There was an interesting quote from one of the spokesman, something to the effect of "The press shouldn't have access to our system". In the meantime the Mr. Zeliff has asked for apologies, etc.

By the third day the duplicate entry was definitely declared a mistake.

Interestingly, the influential (and decidedly Anti-Zeliff) *Union Leader* newspaper of Manchester, NH. decided to stay out of the fray, running only a small sidebar on the issue the second day and one or two short editorials, all of which showed amazing restraint. (The *Union Leader* has an extremely conservative editorial position and has the widest circulation in the state; its statewide influence is considered to be *powerful* by most political observers.) Yesterday's Sunday Edition of the *Union Leader* also included a discussion of the *risks* of such electronic databases; the article mentions EFF and other 'privacy' advocates prominently.

As for the damage to Mr. Zeliff's election chances, the results are still unclear, but seem minimal. His main competitor in the Republican primary did not make an issue of the problem, choosing instead to continue harping on a ``fact-finding'' mission Mr. Zeliff made to South America last Winter (at taxpayers expense, of course).

[I apologize for the sketchiness of this report: I have the newspapers at home and should be able to substantiate some of the more relevant facts when I get home this evening.]

Craig Neth Digital Equipment Corporation 110 Spit Brook Road
ZK03-3/Y25
Nashua, NH 03062 neth@zk3.dec.com

[Apparently the *other* SSN belonged to a four-year-old. PGN]

⚡ Microsoft's warning

MIKE WALSH <mike.walsh@pcb.compart.fi>

Fri, 23 Aug 96 09:43:00 +0200

Thomas Reardon of Microsoft points out that Internet Explorer 3.0 now includes a warning of "suspect" software. The Risk here is that this warning is far too broad. That is you seem to get the warning for almost everything. Thus the typical user will almost certainly get into the habit of pressing the Yes button every time - just as he/she already does on all the idiot "are you sure" prompts. The warning by itself is thus useless. Another Risk is that the user can't distinguish between Intranet and Internet usage. If we assume that on the Intranet he is allowed to download ActiveX modules because they are considered safe there, but now (sorry NOT) allowed to download ActiveX bits from the Internet, how is he able to tell them apart. The browser certainly doesn't. Mike Walsh, Pohjola, Finland

⚡ Microsoft's patch ([RISKS-18.36](#))

Ed Felten <felten@CS.Princeton.EDU>

Fri, 23 Aug 1996 10:29:33 -0400

We have tested Microsoft's patch and have verified that it fixes the problem we reported. The patch is available from

<http://www.microsoft.com/msdownload/iepatch.htm>

⚡ Why Java, Bash, Explorer, and other bugs keep hurting us

Fred Cohen <fbcohen@california.sandia.gov>

Thu, 22 Aug 1996 07:37:07 -0700

This is just an editorial opinion from a non-editor of risks.

We see

increasing numbers of security holes formed from what would appear to be

minor design or implementation flaws in systems - particularly in the

user-level programs running on those systems. Perhaps the real problem

comes from not using trusted systems. Some examples:

Java allows access to user files:

A trusted system could prevent this regardless of any flaws in Java. Just provide it with a private area.

Bash error allows character code ff to act as a separator:

A proper trusted system would not allow you to exploit this to any advantage.

Explorer error lets you overwrite system and other files:

Again a trusted system would eliminate the problem.

Perhaps the real problem we face has to do with the lack of interest by the

community in using technologies that we know about and that are highly

effective in preventing a wide range of threats. Instead of building on the

work of others, people keep on starting from scratch and making the same

mistakes again and again.

Fred Cohen can be reached at tel:510-294-2087 fax:510-294-1225

⚡ Too much integration

+33)88412674 <Nick.BROWN@DCT.coe.fr (Nick BROWN) (Tel>

Thu, 22 Aug 1996 15:49:15 GMT

For a long time, I've been coming to the conclusion that one of the biggest RISKS in computing (and, since that's starting to touch every aspect of our lives, everything else), is an excessive degree of integration. It increases system complexity (read: bugginess) exponentially for often negligible benefits.

A couple of items in [RISKS-18.36](#) bring this home:

> before Explorer downloads a dangerous file like a Word document,

Sorry ? A Word document is dangerous ? Ah yes - when you run it, an auto-start macro buried in the document itself might get DOS to format your hard disk... Why do the 99% of users who just want to edit a letter have to risk their entire system integrity for what is basically a gee-whiz feature ?

(Does Word have some way to load documents without executing any auto-start macros ? Or would that be too complex because users could turn it off and then forget they'd done it when they needed to run an autostart macro ?)

> Friends of mine have a remote-controlled gas fireplace in

their new home.

I tested this statement on several colleagues (all computer people). They all thought it was either (a) "hugely funny" or (b) "absolutely terrifying".

Typical reactions in the respective categories were

(a) "who's so lazy that they want a real, old-fashioned-style, back-to-nature log[-effect] fire, but can't be bothered do something old-fashioned like getting their b*tt [AOL!] out of their chair" [I suppose it may have been an unrequested feature of the house, put in by the builders following input from their "marketing" types - NB]

(b) "every electronic system fails at least once every 5 years or so - to run something as dangerous as burning gas with a 27 MHz [we presume - NB] \$4.99 remote circuit is just insane".

The other day, I was in an electrical store (buying an overvoltage protector...go figure) and the lady in front of me was trying to find a replacement remote control for her shutters. These had been stuck in the down position for two weeks because the remote's cheap push buttons were sticking. If there was a manual override in the house, she sure didn't know where it was.

These days, before buying almost anything, I try to work out what its failure mode is likely to be, how long I can reasonably expect it to (a) work and (b) be reparable. The results of this calculation for personal computers is one of several reasons why I don't own one (but

that's another
story).

Nick Brown, Strasbourg, France

✉ Re: Computer testing of nuclear weapons (Ferguson, [RISKS-18.36](#))

"Frank C. Ferguson" <ferguson@dmapub.dma.org>

Sun, 25 Aug 1996 17:40:47 -0400

On Sun, 25 Aug 1996, A. Lester Buck III wrote:

> >I suspect we would soon be building weapons that would never
> work when
> >the real trigger was actually squeezed.
>
> The very first nuclear weapon was designed (and tested!) using
> teams of
> women operating hand calculators. Funny thing, it worked the
> first
> time!

The very first atomic bomb was tested (and destroyed) in the
desert out
west. The second and third atomic bombs were tested over
Hiroshima and
Nagasaki. Even though the first one worked, most of the
scientists weren't
sure #2 and #3 would work because they were made differently.
One of the
main reasons that a demonstration wasn't conducted for the
Japanese was
because our experts weren't sure it would work. Computers are
very useful
and should be used as much as possible, however, anyone who
thinks that a
computer can reliably substitute for a "real" test is naive.

⚡ Re: Computer testing of nuclear weapons (Ferguson, [RISKS-18.36](#))

Jake Donham <donham@linex.linex.com>

Mon, 26 Aug 1996 14:03:11 -0700

>> to use the new computer ... to determine which country wins a war

>> without actually fighting the war.

Perhaps the best fictional treatment of this idea appears in Philip

K. Dick's "The Variable Man". Dick's works (especially his short stories) contain a wealth of RISKS-relevant ideas.

⚡ Re: Computer testing of nuclear weapons ([RISKS-18.36/37](#))

Mike McKinlay <MMcKinla@dbq.cycare.com>

Fri, 23 Aug 96 08:33:00 PDT

[In response to Frank C. Ferguson's response concerning the ancient Chinese to Jonathan Kamens noting Star Trek's origin of "virtual war"]

"We inwented the ancient Chinese." -- Pavel Chekov

⚡ Year 2000 Bites the Budget

Frank Christensen <frankc@aquila.com>

Thu, 22 Aug 1996 10:53:59 -0500

[Frank sent in a long copyrighted Reuters item, 22 Aug 1996, on the Y2K

problem, citing estimated costs to the U.S. Government of \$9 to \$30

billions, with worldwide fixes costing from \$300 to \$600 U.S. billion.

The article also noted that Nebraska is imposing a two-cent tax per

pack of cigarettes, to help smoke out the state's reprogramming problem.

Independently, Mark Brader forwarded an item from Malcolm Austin

<maus@ms.com>, who had suggested naming a project aimed at this problem

``Dreadnought'', but he was voted down with those preferring

``Odyssey 2000''. In response, Malcolm noted that the original Odyssey

project (Odysseus's voyage) ended up 20 years behind schedule, and

killed off everyone involved except the lead manager. I like Malcolm's

chosen name, but suppose that a fractured American spelling, DreadNaught,

might be slightly more appropriate. PGN]

✉ Re: London train crash (Poole, [RISKS-18.37?](#))

"Clive D.W. Feather" <clive@demon.net>

Fri, 23 Aug 1996 17:19:12 +0100 (BST)

> The northbound train (with the passengers) was the 17:04 which left on time.

> The preceding northbound train (16:54) was delayed by over 6 minutes which

> meant the southbound (empty) train would have been delayed by at least that

> in crossing over onto the other line.

Not necessarily. The signalman would have all three trains visible on his panel. If the other train was that late, the signalman could have crossed the empty train **before** the late train reached the area. This is the sort of thing they do every day.

Clive D.W. Feather, <clive@demon.net> Associate Director, Demon Internet Ltd.
<cdwf@cityscape.co.uk> Director, CityScape Internet Services Ltd. +441813711138

⚡ Re: "Inability to tinker not confined..." (Scott, [RISKS-18.37](#))

"Tom Zmudzinski" <zmudzint@ncr.disa.mil>
Fri, 23 Aug 96 11:35:30 EST

In [RISKS-18.37](#), Alastair Scott <scotta@logica.com> wrote:

> Who was it who wrote that "any sufficiently advanced
> technology is
> indistinguishable from magic"? They are right, and they are
becoming
> more than right.

Answer: Arthur C. Clarke

And Dr. Stanley Schmidt once wrote, "Any sufficiently advanced magic is indistinguishable from technology."

Rhetorically, Tom Zmudzinski

[Also noted by Stanton McCandlish <mech@eff.org>. PGN]

✶ Once more Murphy's Law

Jim Horning <jhorning@ix.netcom.com>

Sat, 24 Aug 1996 11:24:32 -0700

This was in my inbox today, concerning an order scheduled for delivery August 15 (fortunately, I was not in a hurry for it):

```
> Subject:
>      <Firm> order update
> Date:
>      Fri, 23 Aug 1996 09:44:46 -0700
> From:
>      <<person>@<firm>.com>
> To:
>      jhorning@ix.netcom.com
```

```
>Dear Mr. Horning:
>Your order has been processed this morning and will be shipped
out today,
>via Federal Express second day, and you will receive it Monday,
August 26th.
>You will not be charged for shipping. For future reference,
your new order
>number is <number>.
```

```
>All Federal Express and Airborne Express orders that were
processed and
>uploaded to our distributor on Monday, August 12th were subject
to a
>technical error which placed them on a hold without anyone's
knowledge,
>until we started hearing from our customers.
```

```
>Please accept our apologies for this problem, as well as for any
>inconvenience this has caused you. Please let us know if you
have any
>questions or comments.
```

```
>Best regards,
><Person> <Firm>
```

[TECHNICAL ERROR? Is that a human error made by a techie?

PGN]

⚡ Dependable Computing for Critical Applications, Final Call for Papers

Catherine A. Meadows <meadows@itd.nrl.navy.mil>

Mon, 26 Aug 1996 13:36:07 -0400 (EDT)

DCCA-6 Call for Papers
Sixth IFIP International Working Conference on
Dependable Computing for Critical Applications
Can We Rely on Computers?
March 5-7, 1997
Garmisch-Partenkirchen, Germany

Final deadline for original papers is 3 Sep 1996.

Prof. William H. Sanders
University of Illinois Tel: 217 333 0345
CRHC - Coordinated Science Lab Fax: 217 244 3359
1308 West Main Street E-mail: whs@crhc.uiuc.edu
Urbana, Illinois 61801 USA



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 18: Issue 39

Friday 30 August 1996

Contents

- [Qualcomm Satellite Tracking System creates regulatory risk](#)
[Steve Grabhorn](#)
- [911 and voicemail](#)
[Carl Jester](#)
- [Caching in web proxy gateways and content negotiation](#)
[Klaus Johannes Rusch](#)
- [Java passwd changer?](#)
[Ken Bass](#)
- [Risks of lowered expectations of stability](#)
[Daniel P. B. Smith](#)
- [When the muzak goes quiet: risks of exception strategies](#)
[Nick Brown](#)
- [Tunnel vision of Computer Society CD-ROM](#)
[Geoff Kuenning](#)
- [US Army troubled by viruses in Bosnia](#)
[George Smith](#)
- [Re: Denial of service ... Netcom listservers](#)
[Methvin Dave](#)
[Brent Chapman](#)
- [Update on GPS Explosion](#)

[Bob Potter via David Kennedy](#)

● [Karpov Wins Online Chess Match](#)

[Edupage](#)

● [DIMACS Workshop on Network Threats](#)

[Wanglai Li](#)

● [Info on RISKS \(comp.risks\)](#)

⚡ **Qualcomm Satellite Tracking System creates regulatory risk**

Steve Grabhorn <steveo@nosc.mil>

Wed, 28 Aug 1996 23:57:24 -0700

[Here is a case that has considerable RISKS interest because of the potential availability of historical data to regulators. PGN]

Qualcomm Inc.'s popular Omnitronics [Omnitracs?] electronic truck-tracking system is causing tension between regulators and truck lines. The system uses satellites and receivers to give trucking companies two-way messaging with its drivers, as well as accurate data on the location of trucks. The Federal Highway Administration is battling Youngblood Truck Lines of North Carolina over what data Youngblood must provide the regulators. In response, Truckers United for Safety has filed a lawsuit contending that regulators are trying to force Youngblood to retain electronic data from its system for use in audits (with even accidental discrepancies between logged hours and actual hours potentially resulting in fines). Youngblood is considering dropping its very productive use of the system, to avoid the ensuing risks. This is at least the second time federal

regulators have demanded electronic data. Although current regulations do not require it, proposed new regulations do. [Source: Regulators seeking Qualcomm truck data, By Elizabeth Douglass, Staff Writer, *The San Diego Union-Tribune*, 25 July 1996. PGN abstracting.]

🔥 911 and voicemail

carl jester <cjester@interaccess.com>

Wed, 28 Aug 1996 22:38:33 -0500

Last Friday evening, after most people had gone home, the local police arrived at my place of employment in response to a 911 call. There was no message, and the caller hung up immediately. On Monday this happened again, once in the morning and once in the afternoon. The police simply called to check that it was a false alarm. On Tuesday the calls picked up, at one point occurring about 5 minutes apart. By this point the police were becoming upset (I certainly don't blame them).

Due to the nature and timing of the calls, it seemed most likely that there was a problem with a modem. The most obvious choice was a new Win 95 notebook used by a field tech. Win95 keeps track of things like dialing 9 or 1 for you. This combined with a tech entering 9 or 1 as well might cause this (more likely 9191 or 991, although 911 is possible). Unfortunately for that theory, the notebook was configured correctly.

The problem turned out to be a recently (Friday afternoon) deactivated voice mail box. Friday was the last day for one of our sales staff (he is leaving the area). He had set up his voice mail to page him whenever he received a new message. When his box was deactivated, his pager number was deleted. The code he chose to identify voice mail on his page remained. The code was, I'm sure you've guessed by now, 911. Whenever he received a new message the now blank number, followed by the message (911) was sent to the switch.

Risks? First, 911 no longer sent anybody to check on the problem. If we'd had a real emergency, response time would have been slowed. Second, a "denial of service" as 911 operators were busy with us when there might have been a real emergency elsewhere.

Carl Jester cjester@interaccess.com <http://homepage.interaccess.com/~cjester>

⚡ Caching in web proxy gateways and content negotiation

Klaus Johannes Rusch <KlausRusch@atmedia.net>
Sat, 24 Aug 1996 12:46:52 CET

As the architected method for language negotiation between web browsers and web servers is not supported by all products, and often fails as users tend not to customize their browsers properly, attempts have been made to select the preferred language (and sometimes content) based on host names.

Similarly, different versions of a page may be sent depending on the browser's capabilities, the line speed and the like.

Country guessing seems to get much harder with emerging caching strategies.

The two requests below originated at the same client in the .at country domain.

The first one got propagated from proxy.tuwien.ac.at to ebone-proxy.univie.ac.at, and finally to salvator.ecrc.net (with possibly some additional proxy servers in between). In the second has, ebone-proxy.univie.ac.at actually fetched the document.

```
salvator.ecrc.net          - - [22/Aug/1996:14:34:06 -0400]
ebone-proxy.univie.ac.at - - [22/Aug/1996:14:37:03 -0400]
```

Now what's the problem with this? At the server there is no evidence where the request actually originated. The assumption that proxy servers tend to be in the same geography, consequently in the same top-level domain, does not hold any more.

In this case, with a .net domain, most servers will probably present the English version of a document, which may not be the intent of the author, but still acceptable for many users.

With proxy servers being located in different country domains, however, there is a risk of presenting a language version which is very likely not to be understood at all.

Likewise presenting different versions of a document to meet legal requirements such as adding extra disclaimers, or to direct users to

country-specific information, or optimizing for specific browsers, may fail for the very same reasons: The cached version of a dynamically created home page, optimized for use with Netscape and excessively using tables and graphics, was sent to a text-based Lynx client.

Klaus Johannes Rusch e8726057@student.tuwien.ac.at,
KlausRusch@atmedia.net
<http://www.atmedia.net/KlausRusch/>

⚡ Java passwd changer?

Ken Bass <kbass@fred.net>
Wed, 28 Aug 1996 22:48:30 GMT

Excerpts from InfoWorld:

"Courion Corp. has announced Password Courier ... "

"Password Courier integrates with existing help desk systems and allows users to reset their own passwords to networks. "

"Courion estimates that 10-20% of internal help desk calls are from users who have forgotten their passwords or have been denied because of invalid password attempts."

"Users can access Password Courier from a web browser in a corporate intranet and authenticate themselves with personal identification information.

It appears the system is for intranet applications, but I wonder how easy it would be for someone to change my password for me? If this become an automated process, not requiring the human verification and interaction, I'd

be concerned of the risks.

⚡ Risks of lowered expectations of stability

"Daniel P. B. Smith" <dpbsmith@world.std.com>

Thu, 29 Aug 1996 09:40:44 -0400 (EDT)

>From an actual review of a software package, "Personal Engineering," Aug 1996, p. 51: "In general, I really enjoyed working with this package and am impressed with its stability. During the entire review process I only got it to crash twice, and neither situation was repeatable." Can you imagine Consumer Reports saying "We really liked the Frammis sport utility vehicle and were impressed with its stability. During the entire review process we got it to roll over only twice, and neither situation was repeatable."? Or, "We really liked the [xxx airplane]. During the entire review process we got it to crash only twice, and neither situation was repeatable."?

⚡ When the muzak goes quiet: risks of exception strategies

+33)88412674 <"Nick BROWN" <Nick.BROWN@DCT.coe.fr> (Tel>

28 Aug 1996 15:39:33 +0000

A few months ago, my wife was shopping in the supermarket when large lines started to form at the checkout counters. It turned out that (of course) the whole payment system was down.

In this French store, the procedure to be followed in this case is very simple: you wait. I suppose the reasoning goes that even if all the articles had price stickers, and all the checkout people had calculators and/or very good mental arithmetic skills, there'd still be no point in adding everything up by hand since the majority of people would have nothing to pay with apart from their debit cards.

Anyway, after about half an hour, the lines got moving again, and my wife made what turned out to be the right call: rather than dump her trolley and hope that store employees would put all the frozen stuff back in the freezers before bacteria decided to wake up and multiply for the next customer, she made it through the line and was able to pick the children up from school only a couple of minutes late.

I assumed this was pretty much all a store could do in this kind of case, until I was in a Safeway supermarket in Britain last month [I think Safeway UK is completely independent of Safeway US - NB]. While waiting in line at the checkout, I was idly reading one of those stand-up signs that says something like "to serve you better, this counter is closed", which was waiting to be deployed on some unsuspecting victim. When I turned it over, however, I found another message, indicating that this supermarket chain, at least, is prepared for when technological Armageddon strikes. Here (approximately) is what it said:

"Owing to a technical problem, we are unable to process purchased items electronically. Therefore, your bill will be calculated by multiplying the number of items in your basket by an average item price. Thank you for your understanding."

Now, I presume this must be legal, because I said jokingly to the clerk "I bet you hope that never happens" and he said "It happened when I was on duty a few months ago". Apparently the average item price (I wonder if this is the average price of each stocked item, or a weighted average of what people purchase) is around 94 pence, say US\$ 1.42. When the big moment comes, you get the choice: pay the average price, or drop everything and leave the store.

So, next time you're in Britain and the lights go low in the supermarket, the message is clear. Empty your trolley of canned vegetables and head for the electrical goods and alcoholic beverages section.

The RISKS are numerous: huge financial losses for the store as savvy comp.risks subscribers empty the shelves of foie gras and champagne; confrontations between customers and clerks over the bill; and the store (inadvertently) ripping you off if you just have to buy a pint of milk and a small loaf of bread, right now.

⚡ Tunnel vision of Computer Society CD-ROM

Geoff Kuenning <geoff@ficus.cs.ucla.edu>

Wed, 28 Aug 1996 12:12:24 -0700

I just posted the following to comp.org.ieee, and consider it appropriate for RISKS as well:

Since I subscribe to about 7 IEEE Computer Society publications, which take up significant shelf space, I was excited to learn of the new CD-ROM with all of 1995's issues on it. To learn more, I visited the Computer Society's Web site (www.computer.org).

The first disappointment was the difficulty of even finding the proper sub-page (their search engine won't let you look for punctuation or "words" of 2 letters, so I was reduced to looking for "ROM" and hoping I wouldn't get lots of hits about ICs). But this was nothing compared to the discovery that the \$90 CD-ROM would be a waste of my money.

Why is this true? The CD-ROM stores articles in SGML format, together with a database to help you search it. SGML viewers are provided for the Mac, Windows 3.1, and "Unix". Note that SGML is a superset of HTML, so that common Web browsers won't display the files correctly. Worse, the "Unix" variants supported by the viewers and the database engine are SunOS, Solaris, and SGI IRIX -- **only**. Users of DEC Alphas, Linux, Nexts, most popular x86 Unixes, etc., are out of luck. So are Windows NT users, who have already raised complaints about incompatibility.

But if you think the audience is limited now, consider the potential

lifetime of the CD-ROM. The UCLA library keeps 10-30 years of IEEE publications on the "active" shelves, and a complete history in secondary storage. My own collection is smaller but still dates back quite a few years. What are the chances that, 30 years from now, we will be able to run this software? The data will be there, and there's a good chance that there'll be hardware capable of reading the now-obsolete CD-ROMs. But I doubt that Windows 3.1 will be around.

The IEEE Computer Society has stumbled twice here. First, as a society of computer scientists, it should not be disenfranchising its members by publishing data that can only be viewed with proprietary software. Second, the choice of formats and software has been excessively focused on the technology of 1995, with little apparent planning for the libraries of the 21st century.

I recognize that the IEEE cannot afford to support every oddball operating system out there, let alone predict the future. It is for precisely this reason that they should have made the CD-ROM available with complete documentation and source code included, so that all potential current and future customers would have an equal chance to make use of the information therein.

Geoff Kuenning g.kuenning@ieee.org geoff@ITcorp.com
<http://fmg-www.cs.ucla.edu/geoff/>

✶ US Army troubled by viruses in Bosnia

George Smith <76711.2631@CompuServe.COM>

Wed, 28 Aug 1996 23:03:52 +0000 (GMT)

PGN-excerpted from VIRUS-L Digest Friday, 30 Aug 1996 Volume 9 : Issue 152

Date: Fri, 30 Aug 1996 23:09:31 +1200 (NZT)

From: virus-l@cantva.canterbury.ac.nz

Subject: VIRUS-L Digest V9 #152]

Administrative mail to n.fitzgerald@csc.canterbury.ac.nz.

Posting guidelines <ftp://CS.UCR.EDU> ; FAQ at <ftp://cs.ucr.edu/pub/virus-l>

Writing in an article entitled "US Army Seeks Computer Antivirus Plan" in the 26 Aug 1996 issue of *Defense News* magazine, reporter Pat Cooper reveals the US Army suffered from serious computer virus infections while deployed in Bosnia.

Infections by Monkey, AntiEXE and Prank Macro caused computer software malfunctions and related problems which "forced Army personnel to waste hundreds of hours finding the viruses and cleaning them from the systems..." Apparently, imperfect Monkey virus removals also resulted in non-critical data being lost from infected hard disks.

The widespread dispersal of the viruses on Army computers in Bosnia have catalyzed a review of information systems procedures and could have implications for all future force deployments, servicewide, according to Cooper and *Defense News*.

Army Captain Steve Warnock told Cooper that while virus computer trouble

was widespread, it affected only "nonsensitive data and did not adversely affect the Bosnian mission."

Army officials pressed for solid recommendations that all computers be checked for computer viruses prior to future deployments. One suggestion aired involved the maintenance of an on-line site from which Army personnel could download current anti-virus software while in the field.

Pat Cooper commented to Crypt Newsletter that the US Army had used IBM Anti-virus and McAfee Associates software while in Bosnia. Crypt Newsletter <http://www.soci.niu.edu/~crypt>

[Tails from The Crypt. PGN]

✶ Re: Denial of service ... Netcom listservers (Markowitz, [RISKS-18.38](#))

Methvin Dave <dmethvin@cmp.com>

Fri, 30 Aug 1996 11:04:48 -0400

Let me provide a victim's perspective on Netcom's mail list troubles. I was one of about two dozen people who were falsely subscribed to over 1000 mailing lists in the early hours of 10 Aug 1996 by someone calling himself "johnny xchaotic". On 12 Aug, the mail bomber posted a manifesto in news.admin.net-abuse; you can find a copy of it at <http://www.winmag.com/people/dmethvin/mailbomb.htm>.

The good news as far as RISKS goes was that there were hundreds of mailing lists that did the right thing and rejected the subscription

request. Some mail list software detected the inconsistency between the From address and the rest of the header. Others realized that the sheer number of simultaneous subscriptions reeked of spam. Others sent a confirmation request that had to be returned to start the subscription; I deleted them and the subscription never got started. Ahh, the beauty of well-behaved software.

Netcom's mailing list software (and many others as well) fell into the other category. It was suckered by the forged From in the header, wasn't at all troubled that the attacker was asking to be signed up to every list at Netcom, and didn't send any confirmation request before adding me to the list.

By the time I logged on later that Saturday (about 10 hours after the attack started), I had over 1600 mail messages. Since I was going on a long business trip that week, followed by a vacation the next week, I knew I wouldn't have time to deal with the problem immediately. I decided to have my incoming Internet mail turned off at our corporate gateway, so that messages to dmethvin@cmp.com would be bounced back to the sender. In attempts to contact them, I found out that many of the other victims are also bouncing mail, some because their mailboxes are full.

In the case of Netcom's mailing list, I suspect that since our bounced messages went back to their mailing list address, the software just turned them back around and sent them to the mailing list distribution

again,
including all the people who couldn't accept mail. And guess
what? The
messages bounced again and again and again. There was nothing
malicious that
I or any of the other victims needed to do to cause this loop,
but if it
gets Netcom to straighten out their mailing list software then
it's a good
thing.

Dave Methvin, Executive Editor, Windows Magazine dmethvin@cmp.
com

[I guess that Dave can never have a WinDoze. PGN]

✶ Re: Denial of service ... Netcom listservers (Markowitz, [RISKS-18.38](#))

Brent Chapman <Brent@GreatCircle.COM>

Mon, 26 Aug 1996 20:48:32 -0600

I don't know anything about this incident or about Netcom's
installation of
Majordomo (the mailing list management software in question),
but speaking
as the original author of the software, let me quote the
original design
paper ("Majordomo: How I Manage 17 Mailing Lists Without
Answering
'-request' Mail", USENIX LISA 6 conference, 1992):

... the goal is not absolute security, but to avoid people
making a nuisance of themselves by abusing the Majordomo
server.

By today's standards, Majordomo's "security" measures are
incredibly weak;
they weren't particularly strong even 5 years ago, when the

software was written. Most lists are configured so that users can subscribe or unsubscribe themselves, which is determined simply by checking that the "From:" line in the header matches the address they're trying to subscribe/unsubscribe, and thus trivially subject to forgery. Furthermore, those operations that are "protected" are accessed through reusable passwords sent in clear-text through e-mail, and thus trivially subject to interception and reuse.

The next release of Majordomo (which will be version 1.94) will include a simple challenge/response "confirm" mode for lists, where a supposed subscriber will be sent pseudo-random confirmation string that they must turn around and send back to the server before their subscription is finalized. This should significantly cut down on the spam subscriptions. Version 1.94 is in alpha test now, and due for release sometime in the next few months; send e-mail to majordomo-announce-request@greatcircle.com if you'd like to be added to the list for notification when it's released, or to majordomo-workers-request@greatcircle.com if you're interested in helping with the development and alpha/beta test)

Clearly, I should have worked harder to keep folks from making a nuisance of themselves with the original version of Majordomo. Some days, I think that releasing the damn thing was the biggest mistake I ever made... :-)
And I now have a lot of sympathy for folks like Eric Allman (author of Sendmail), whose creations have taken on a life of their own on the net...

Brent Chapman | Great Circle Associates | 1057 West
Dana Street
Brent@GreatCircle.COM | <http://www.greatcircle.com> | Mountain
View, CA 94041

[RISKS is greatly indebted to Brent and majordomo. They have greatly simplified my life, and will do even more in 1.94. The challenge-response will also get rid of the jerks whose FROM: addresses are flagrantly unanswerable; on 28 Aug alone, I had to manually remove four would-be new subscribers whose given addresses bounced on the acknowledgement, and I had one more just before putting this issue out! PGN]

⚡ Update on GPS Explosion

David Kennedy <76702.3557@CompuServe.COM>
29 Aug 96 09:40:12 EDT

C4I-Pro-Digest Tuesday, August 27 1996 Volume 02 :
Number 458

Date: Mon, 26 Aug 96 09:54:00 +6
From: Potter B MSgt ACC/SCXX <potterb@ns.langlely.af.mil>
Subject: c4i-pro Update to PLGR Battery Venting Event

Potter B MSgt ACC/SCXX <potterb@ns.langlely.af.mil>

Here's an update on the exploding Precision Lightweight GPS Receiver:

Regards,

//Bp//

(<http://www.geocities.com/Heartland/7167/>)

MSgt Bob Potter (potterb@hqaccsc.langlely.af.mil)

HQ ACC/SCXX (DSN 574-5736)

- - - - -
Issues:

- (1) AA battery tray safety of use
- (2) Is PLGR battery venting event systemic or anomalous? (i.e. design or manufacturing related)
- (3) Is there anything that the operators can do to minimize chances of reoccurrence?

Discussion:

This issue for us is no longer a singular matter of finding out what happened to cause the violent venting at Fort Irwin on 29/30 July 96. We hope to be able to determine what the exact cause of that violent venting was, however, there could be a number of contributing factors and we may never know exactly what caused that violent venting. The bigger issue is what are we learning from the on-going testing as we try to determine what could have caused the violent venting at Fort Irwin, and given this learning, what can we tell users of the PLGR that will prevent a reoccurrence of this type of incident in the future.

[DMK: Discussion of batteries, diodes and case specification deleted.]

Summary: The investigators cannot replicate the explosion through single failures or combinations.]

Recommendation:

Until further notice, if operating PLGRs with external power, remove prime power battery. This includes BA5800 lithiums and AA lithium batteries when used with AA battery holder. The use of AA alkaline batteries

when used with
the AA battery holder is safe, even if holder deforms. In other
words when
operating on external power the prime power battery compartment
should not
contain any lithium batteries!!!

Dave Kennedy CISSP Lead InfoSec Analyst InfoSec Recon NCSA

[Die,lithium batteries? (See [RISKS-11.95.](#)) PGN]

🚀 Karpov Wins Online Chess Match (Edupage, 27 August 1996)

Edupage Editors <educom@elanor.oit.unc.edu>

Tue, 27 Aug 1996 19:51:39 -0400 (EDT)

In an open chess game on the Internet, Russian grandmaster
Anatoly Karpov
defeated several hundred opponents in a game that lasted 65
moves and four
and a half hours. For each move, contestants had seven minutes
[down from
the originally advertised 10 minutes, at Karpov's request -- I
guess he did
not want to get too bored. PGN] to indicate their response, and
a computer
calculated the most frequently suggested response. (*The New
York Times*,
27 Aug 1996, B9) [See <<http://www.tele.fi/karpov/gameworl.htm>>.]

[This item is noted primarily for archival purposes, as a
follow-up
to the risks suggested in [RISKS-18.37](#). The result was clearly
not
a surprise. Only about 300 hundred opponents? Suppose the
group was
composed of only a few grand masters? What would that do to
the odds?
Better yet, one grand master with others kibitzing by e-mail.

If a
grand master can play simultaneous matches, it should be no
difficulty
winnowing the e-mail suggestions in real-time.

I suppose at the next Computer Chess Olympics we will see on-
line groups
of Russian chess players pitted against their U.S.
counterparts using
this software, *en mass-ant*. PGN]

⚡ DIMACS Workshop on Network Threats

Wanglai Li <wli@dimacs.rutgers.edu>

Thu, 29 Aug 1996 14:40:56 -0400

DIMACS Workshop on Network Threats (abridged announcement)
Sponsored by the DIMACS as part of the 1996-97 Special Year on
Networks

4-6 December 1996

DIMACS Center, CoRE Building, Rutgers University

Organizers:

Rebecca Wright, AT&T Research, rwright@research.att.com

Peter Neumann, SRI International, neumann@csl.sri.com

Steve Bellovin, AT&T Research, smb@research.att.com

As the use of computer networks, and in particular the Internet,
has
increased, so has the potential threat to security. In the last
several
years, we have seen numerous security-related attacks on
Netscape, Java, and
the Internet protocols. New protocols and systems for electronic
commerce,
secure financial transactions, and other applications are being
introduced,
and are being deployed quickly, and on a large scale. This
workshop aims to
bring together theorists and practitioners working in areas

related to network security in an informal setting to foster discussion regarding the nature of the threat and what we, as researchers, can do to help manage it.

This workshop will cover topics including, but not limited to:

- o attacks on network security
- o prevention/detection of attacks
- o threat models
- o threats to individual privacy
- o risk management
- o formal methods of security analysis
- o political, legal, and social aspects of network security

INVITED TALKS: Confirmed invited speakers (subject to change) include:

- o Bill Cheswick (Bell Labs)
- o Ed Felten (Princeton University)
- o Peter Neumann (SRI International)

Abstract submissions *by 16 Sep 1996* should describe original, unpublished work, and should be 1-2 pages in length. Abstracts should clearly state the problem being addressed, the nature of the solution, and the main contribution of the work. Abstracts will be selected on the basis of originality, significance, technical content, and applicability. Please include a cover letter indicating the name, address, and e-mail address of the contact author. Electronic submissions are preferred. To submit electronically, send postscript or plain ASCII text to: rwright@research.att.com.

To submit hardcopy, send three (3) copies to:

Rebecca Wright
Network Threats Workshop

AT&T Research
Room 2T-314
600 Mountain Avenue
Murray Hill, NJ 07974

More Information: For more information about the Special Year on Networks,
see the DIMACS web pages at <http://dimacs.rutgers.edu> and for
information
regarding author schedules, registration, travel and local
arrangements for
this workshop see <http://dimacs.rutgers.edu/Workshops/Threats>.
E-mail to
dimacs-www@dimacs.rutgers.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 18: Issue 40

Tuesday 3 September 1996

Contents

- [Accidental missile launch: color-code mixup](#)
[Ken Wood](#)
- [About 3 weeks with network problems...!!!](#)
[Isaias Callejas](#)
- [A funny thing happened on the way to the bank...](#)
[Andy Piper](#)
- [Changing credit-card address](#)
[Gene M. Stover](#)
- [Back-country technology](#)
[Andrew Duane](#)
- [FedEx monitoring of cellular phonecall locations](#)
[Bernard Glassman](#)
- [Re: "More power to us"](#)
[Ralph Barone](#)
- [Algol passwd changer?](#)
[Marianne Mueller](#)
- [Risks of multiple HTTP standards](#)
[Pete Bentley](#)
- [Re: Tunnel vision of Computer Society CD-ROM](#)
[Geoff Kuenning](#)

[Theodore Y. Ts'o](#)

[Timothy R Prodin](#)

● [Re: Exploding GPS \(RISKS-18.39\)](#)

[Matt Fichtenbaum](#)

● [Re: Karpov v. the Internet" game](#)

[Dick Mills](#)

[Pete Mellor](#)

● [19th Information Systems Security Conference](#)

[Jack Holleran](#)

● [Information Security Conference - Cleveland](#)

[Robert Terry](#)

● [Info on RISKS \(comp.risks\)](#)

⚡ Accidental missile launch : color-code mixup

Ken Wood <kenwood@ti.com>

Fri, 30 Aug 1996 12:00:09 -0500

The never ending saga of technology + human error = disaster:

Inquiry Ordered in Missile Incident
STEWART BELL, *Vancouver Sun*

The Canadian navy mistakenly launched an unarmed missile at a town near Victoria, B.C. on Thursday, hitting a residential garage and narrowly missing a food store and day care centre. Sailors were testing weapons systems aboard the HMCS Regina at 11 a.m. when the missile was fired at the town of View Royal on Vancouver Island. The military has since suspended all such testing on both coasts and ordered an inquiry. Although nobody was injured, residents of the bedroom community of 6,000 people say things could have been much worse. Thirty-two children were a half-block away at

the Tiny Tots Day Care Centre when the incident occurred.

HMCS Regina, one of Canada's new \$1-billion high-tech frigates, was docked

at CFB Esquimalt on Vancouver Island during the mishap. A military

official blamed human error, saying a sailor inserted a live missile instead

of a dud into the launcher. The error apparently resulted from a mix-up

over the color-coding of the missiles. While the test called for a green

"inert test set," which contains no propellant and therefore could not

launch, a blue "inert practice round" was mistakenly used.

Neither the missile that was fired, nor the one that was supposed to have

been fired, contained explosive materials. But the errant missile

- 1.5-metres long and weighing 18 kilograms - struck with considerable

force, punching a hole in the garage roof and passing through a workbench before exiting the building and burying itself deep in the lawn.

The story says it all, no commentary needed!

Source: http://www.southam.com/vancouver_sun/

⚡ About 3 weeks with network problems...!!!

Isaias Callejas-SYC <isma@sycmail.syc.com.mx>

Fri, 30 Aug 1996 11:23:25 -0600 (CST)

About 3 weeks with network problems [resulted] when on an "enchanted" day

somebody connected an Ethernet transceiver AUI-UTP over the net with the

Heartbeat Switch enabled.

There are two switches located on the top of the unit: the Heartbeat Enabled (HBE) switch and the Link Test (LNK) switch. The switches are initially set to both Heartbeat and Link test "Enabled".

In the Heartbeat enabled position, the transceiver send a signal (called a "heartbeat") across the AUI collision pair (COL) immediately after it transmits. In the disabled position, a heartbeat is not sent back to the attached device.

The manual says that if the transceiver is attached to a repeater you have to place the switch in the disabled position. Otherwise, the heartbeat signal will falsely indicate collisions to the repeater.

The risks I see are :

- * The transceiver was connected to a PC over the net WITHOUT read the network board's manual of the PC and transceiver, and as the HBE is enabled by default...

- * The risk begin when somebody do something that can affect to everybody without tell it to anybody...!!!

My questions are :

- * Is it necessary to have the HBE enabled by default from factory..???

- * Is more common to need the HBE enabled than disabled...???

The problem was already solved and we spent a lot of time trying to do it.

E. Isaias Callejas Mancilla Sistemas y Computadores de Gestion

Luis Kuhne #10, Col. Las Aguilas C.P. 01710, Mexico D.F. (525)
664 00 96

✶ A funny thing happened on the way to the bank...

Andy Piper <andyp@parallax.co.uk>

Mon, 2 Sep 1996 17:02:16 +0100

Not a new subject to RISKS readers, but a personal experience that amazed me could happen.

I went to our local ATM to get some cash to pay the plasterer last week. I requested 110 pounds, the machine said "please take your money", nothing appeared, then it said "please take your receipt", nothing appeared. I rushed into the bank, they checked it on the computer and yes it appeared to be a valid transaction and yes it had been debited from my account. As it wasn't a branch of my bank I have had to fill in a disputed transaction form to try and claw the money back.

This of course is the age old risk of the computer says its true so it must be :). However, we usually associate problems with ATM's with malicious intent rather than software bugs. For I realised what the problem was - when I used the ATM I initially pressed proceed without entering an amount. The machine then reported the error and asked me for the amount. I am convinced that the "unusual" input conditions triggered a software bug, and sure enough when I tried again entering the right amount straight off I was

presented with the cash, although by this time I was 220 pounds the poorer.

I am just shocked that it was this easy to confuse a simple piece of software/firmware, where the result is rather painful.

I assume that they count the ATM delivery every night so that I **will** eventually get my money.

andy piper andyp@parallax.co.uk

✶ Changing credit-card address

"gene m. stover" <gangrene!gene@netcom.com>

Fri, 30 Aug 96 22:36:31 -0500

I know we've already seen incidents like this, but I thought I'd mention it for the record:

I recently moved and called my credit card company to inform them of my new address. To verify that I was who I claimed, they asked me for the last four digits of my social security number, which I supplied.

Of course, their records didn't agree.

The clerk and I discussed for a while how I could prove my identity. In the end, she said she would change my address now if I agreed to call during the next business day to work out the discrepancy with my social security number.

But it gets better.

I called during business hours the next day to give them my true social security number. Of course, they needed to verify that I was who I was, so the clerk asked me for my address.

The risks? Let me count the ways ...

gene m. stover (gene@CyberTiggyr.com)

⚡ Back-country technology

Andrew Duane USG/PE <duane@zk3.dec.com>

Tue, 3 Sep 1996 10:10:08 -0400 (EDT)

>From the GORP section of the September 1996 issue of the AMC (Appalachian Mountain Club) *Outdoors* magazine:

Clueless:

When two Pennsylvania hikers discovered they were lost in the White Mountain National forest this summer, they tried to use their spiffy high-tech Global Positioning System (GPS) [receiver] to get un-lost -- only the darn thing turned out to be pretty useless without a map. No matter, the hikers simply dialed for assistance on their cell phone. Luckily, officials who fielded the call had not only a GPS, but a map, too, and located the hikers.

Andrew L. Duane (JOT-7) Digital Equipment Corporation
duane@zk3.dec.com (603)-881-1294

✈ FedEx monitoring of cellular phonecall locations

<glassman@sunsite.unc.edu>

Mon, 2 Sep 1996 22:24:13 -0400 (EDT)

A week or so ago I used my Cellular One phone to call FedEx to inquire about Saturday pickup locations near Boone or Blowing Rock NC. At the time, I was nowhere near either of those places, so I did not bother to mention my current location to the operator. The next day, Saturday, I called FedEx with the same cell phone from Blowing Rock to arrange the pickup. The operator immediately asked if I wanted them to come to the intersection that I had placed my call from the day before.

Two days later, a FedEx operator confirmed that they are getting "new systems" at some locations that are able to record the locations from which cellular calls are placed.

I have now asked Cellular One three times to explain to me why they do not tell subscribers that they pass this location information through the system, but to no avail. Each person I talk with says that he or she has never heard that this information is available,

1. Is it just me, or does it seem to other readers that there are legitimate concerns about RISKS to cell phone subscribers who are not warned that they may be having their locations monitored?

2. Is it possible for FedEx to capture information that Cellular One doesn't

know it's passing?

Bernard Glassman

✉ **Re: "More power to us" ([RISKS-18.32](#))**

"Ralph Barone" <Ralph.Barone@BCHydro.bc.ca>

Wed, 14 Aug 1996 11:07:09 -0700

[This message was intended to have been included earlier. It is offered

now as presenting some useful background on the 10 August power outages.

PGN]

In my personal opinion (not that of my employer), there are some factors that contribute to outages like this.

1) The transmission system (the lines between substations) is constructed with more redundancy than the distribution system (the lines from the substation to your house). As a result, the transmission system tends to be more reliable than the distribution system and most failures on the transmission system do not result in loss of service to customers. Usually, when you have an outage at your home, it is because of a fault on the distribution system.

However, the transmission system is built on a much larger scale than the distribution system. Also, when redundant systems finally fail, they tend to fail in a much more spectacular fashion than non-redundant systems.

Therefore, when an outage is due to transmission problems, it tends to be a BIG outage.

2) Utilities, like any other business, are in business to make money. To make more money, you should own as few assets (lines, generators) as possible, utilize it as heavily as possible (to maximize sales) and keep other costs low (small staffs and extended maintenance intervals). This is counterbalanced by pressures from regulatory agencies and customers to provide reliable service. The opening up of the wholesale electricity market in North America is putting greater pressure on electric utilities to be profitable. This tends to push the balance point towards the side of unreliability.

A similar thing has happened in the long distance telephone market. AT&T originally lost customers over price, but is recovering customers on the basis of convenience and reliability. The electric power market appears to be going through a phase similar to the early days of competitive long distance telephone service.

3) Western Systems Coordinating Council (the coordination council for Western US/Canada) regulations mandate that each utility must have 10% extra generation or "Spinning Reserve" available in the event of a system disturbance. For example, if the utility is presently generating 1000 MW, it must be able to bring an additional 100 MW on-line within a certain period of time (1 - 3 minutes, I believe). Power brokers have

recently started buying selling reserve, aggregating it into a pool and selling it from the pool back to utilities. For example, if utility A requires 100 MW of spinning reserve, but the only generator they have that isn't already generating is 200 MW, they can now either:

- buy 100 MW of reserve from the pool and take their generator off standby (perhaps for maintenance).
- leave their generator on standby and sell 100 MW of spinning reserve to the pool, allowing some other utility to take a 100 MW generator off standby.
- buy 120 MW of reserve from the pool, put their generator on-line and sell 200 MW on the open market.

The net effect of this is a reduction of total spinning reserve due to the better fit of each utilities individual resources into the larger spinning reserve pool. This gives the system a smaller buffer in the event of an emergency and increases the chances of outages cascading.

Ralph Barone, Protection & Control Manager/HVDC Control Engineer
BC Hydro Ralph.Barone@bchydro.bc.ca

✶ Algol passwd changer? (Re: Bass, [RISKS-18.39](#))

Marianne Mueller <mrm@Eng.Sun.COM>
Tue, 3 Sep 1996 10:20:04 -0700

The article in RISKS titled "Java passwd changer?" caught my attention, but

the surprising discovery was that this article has nothing to do with Java.

The author speculates about the risks of an automatic password changer, but there isn't one being used today that is causing him to worry. Of course, such a system could be written and deployed in any language. But it couldn't be written and deployed as a Java applet, since the default Java applet security policy prevents applets from reading or writing to the client disk.

I'm not sure what the moral of the story is, but I do know that since the RISKS list is archived all over the place, Java will now show up on search engines with the title "Java passwd changer?" and no doubt people will start writing "USA Today"-style articles about the danger of Java changing passwords!

It may be that the biggest Internet security risk right now is that it's getting harder and harder to find accurate information about computer-related risks.

Marianne JavaSoft engineering, security <http://java.sun.com/people/mrm>

⚡ Risks of multiple HTTP standards

Pete Bentley <pete@mimir.com>
Tue, 03 Sep 1996 15:37:16 +0100

The Microsoft Network offers a free service allowing people to create their

own custom 'start' page at <http://www.msn.com/> which may contain personal information including the individual's address. All of this information is encoded into a 'cookie' which is stored by the user's own web browser and so in theory cannot be seen by other people. Or can it?

MSN uses Microsoft's own product, Microsoft Internet Information Server 1.0, as its web server and it tries to send a response which will ensure that <http://www.msn.com/> is not cached by any proxy servers (to prevent people seeing each others information by mistake), but is cached by the users web browser for a short time (for speed). It does this by sending an HTTP/1.0 reply with Date and Expires headers which indicate that the information is valid for half an hour and adds a "cache-control: private" header to prevent any proxy servers from caching the information. However, cache-control is a header from the draft HTTP/1.1 specification which is not interpreted by many HTTP/1.0 proxy servers in use today (verified by myself with the CERN and Squid proxies) and so is ignored. The remaining headers indicate to the proxy that it may cache the page itself for half an hour. If the proxy then caches a page containing a user's personal information then any other user accessing <http://www.msn.com/> via that proxy in the next half hour will receive that page (and personal information). This scenario has indeed been observed in practice with a busy web proxy run by a large ISP and a detailed analysis has been sent to Microsoft for their attention.

The risk here seems to mostly be mixing HTTP standards and

assuming that
HTTP/1.0 servers will understand some HTTP/1.1 headers. It
raises issues for
both server coders and cache coders as the Net starts gradually
migrating to
HTTP/1.1 at the same time as 'smart' web servers (generating
pages on the
fly) want finer control over caching proxies.

Pete

[Aside: whilst making HTTP requests by telnetting to www.msn.
com:80

(to compare headers), I noticed that www.msn.com either
restarts

(connection refused) or goes missing (routing loops between
msn.net

routers) quite frequently.]

✶ Re: Tunnel vision of Computer Society CD-ROM (Kuenning, [RISKS-18.39](#))

Geoff Kuenning <geoff@ficus.cs.ucla.edu>

Fri, 30 Aug 1996 12:42:22 -0700

Only moments after the appearance of my complaint about the
short-term
usability of the IEEE Computer Society CD-ROM, people started e-
mailing me
to defend the decision to use SGML. Rereading my posting, I
realized that I
did not make myself clear. I do not object to the choice of
SGML as a
format; to the contrary (without having had the time to read an
SGML spec) I
suspect that it was a very wise choice.

My problem is two-fold. First, the software to view the
articles on the
disc was provided in a very short-term format, and one that

disenfranchises

a large fraction of the potential customers. (To publicly answer a couple of private suggestions, I do not think that I should have to go out and browse the net to get this software, nor do I think that it would have been any better to have included an emacs viewer as well as those already present.)

The second problem, which I somehow omitted from my previous message, is that the software to search the database is proprietary. So even if I download an SGML viewer from the net, I can only display articles, and can't take advantage of the nifty search features that ought to be available to everyone.

No solution is acceptable if it depends on external capabilities other than the ability to read simple ASCII from the CD-ROM. Bootstrapping by compiling is OK, and it's OK to provide pre-bootstrapped software for common platforms. But I doubt that any of those platforms will be common 30 years from now, so the Computer Society should have provided for this possibility.

(Incidentally, Software Practice and Experience made the same mistake a year or two ago, except that they limited themselves to Windows 3.1. I contacted them at the time, and received a polite response that resulted in no action.)

Geoff Kuenning g.kuenning@ieee.org geoff@ITcorp.com
<http://fmg-www.cs.ucla.edu/geoff/>

[RISKS received messages on this topic from
jdzik@aol.com (JDzik),
ajm@mcs.com (Alan Miller),
Matthew Wojcik <woj@ccs.neu.edu>,
tprodin@ford.com (Timothy R Prodin),
"Theodore Y. Ts'o" <tytso@MIT.EDU>,
Al Stangenberger <forags@nature.berkeley.edu>. Al noted
that

"This is a widespread problem, though. I try to convince
users that

using Excel spreadsheet format for long-term archival
storage of data

is not a very good idea."

Geoff's message more or less summarizes much of the
discussion, but the

following messages from Ted Ts'o and Timothy Prodin seem
worthy of

inclusion, even if somewhat redundant, as representative of
these

responses. PGN]

[Re: Tunnel vision of Computer Society CD-ROM \(Kuenning, RISKS-18.39\)](#)

"Theodore Y. Ts'o" <tytso@MIT.EDU>

Fri, 30 Aug 1996 16:01:44 -0400

Actually, storing its articles in SGML was the right choice for
the IEEE to
have made. The reason for this is that SGML is a platform
independent
format --- SGML, or "Standard Generalized Markup Language" is an
ISO
standard ISO 8879:1986. While the CD-ROM may have only had
viewers for
Macintosh, Windows 3.1, and a few Unix platforms, it's much more
likely that
an article formatted in SGML will have viewers available on
other platforms

than, (for example) if the articles were stored in Microsoft Word format.

A few more words about SGML. What's really good about SGML is that it is designed to deal with *structured* text. You don't specify things like "Times-Roman-Italics, 10 point"; instead you specify "book title", and leave it to the SGML viewer to put the text of the book title in the appropriate font. This is important, because different platforms have different fonts available to them; and 100 years from now, who knows what fonts will be available by default.

An SGML document has a prologue where it declares its Document Type Definition (DTD). The Hypertext Markup Language (HTML), which is used by the Web, is a DTD. Other examples of SGML include the QWERTZ DTD, which provides most of the facilities of LaTeX, and the LinuxDoc SGML, which is derived from the QWERTZ DTD, and which is the standardized format for the Linux Documentation Project (LDP). The LDP has provided Linuxdoc-SGML translators which will take the Linuxdoc-SGML and translate it into LaTeX, groff, HTML, and texinfo. (And of course, from all of these formats, you can then get postscript or Adobe PDF).

So the mere fact that the IEEE CD-ROM is using SGML does not mean that they have "stumbled badly". What's really important is what DTD did they use to format their articles, and is that DTD documented so that other people can write their own SGML translators. Of course, it would have been best if the

IEEE could have provided the source to the SGML translators, but there may have been licensing issues barring them from doing so.

Could you use raw ASCII text instead of SGML? Of course. However, you would lose all the nice formatting that you would get if you were reading the article in printed form. Things like diagrams and graphics would be lost. The advantage of using SGML is that all of this information is preserved, and assuming that the definition of the DTD is public, it shouldn't be difficult to write a SGML -> raw text translator. It would no doubt lose information during this transformation, but that's what you get if you insist on viewing things using raw text.

Ted

[✂ Re: Tunnel vision of Computer Society CD-ROM \(Kuenning, RISKS-18.39\)](#)

Timothy R Prodin <tprodin@ford.com>

Tue, 3 Sep 1996 10:31:22 -0400 (EDT)

In [RISKS-18.39](#), Geoff Kuenning pointed out some problems with the IEEE Computer Society publications on CD-ROM. I would like to correct a mistake and some perception problems that appeared in his article.

First, SGML is not a superset of HTML. SGML is a meta-language that is used to describe content models for documents. Various flavors of HTML are implementations of SGML; with the notable exception of Netscape

3.0.

The tool that IEEE provides for viewing the collection is EBT's DynaText; but because a conforming SGML document instance is tool independent, you can get many different viewers for many different platforms and not have to worry about tool compatibility. You can even construct your own viewers/publishers/search engines, use DSSSL to provide online or paper formats for the instance, and standard tools to perform transformations into other DTDs, such as HTML 3.2.

[...]

IEEE did not disenfranchise their members or customers. An SGML instance is not based on proprietary software; it is in fact based on the complete opposite, a recognized international standard, ISO8879. There exists many tools in the public domain and commercial markets for viewing, manipulating and transforming instances.

Second, the choice reflects lots of planning for technology of the 21st century. There exists a commitment from ISO to keep any modifications to the standard backwards compatible with the current version. Because the standard is in the hands of an international body and not a corporation (such as Netscape's HTML; or Microsoft's RTF) there is a guarantee that changes to the standard will be made only with public comment, public notification, and reference implementations.

It is precisely because IEEE cannot predict the future that they selected a

document format that will insulate them from various operating system quirks, future changes, and emerging technologies.

⚡ Re: Exploding GPS ([RISKS-18.39](#))

Matt Fichtenbaum <mattf@harpa.ultranet.com>

Fri, 30 Aug 1996 19:47:17 GMT

At my last employer we once had a lithium battery explode. Maybe it's the same phenomenon.

The battery in question preserved calibration data in a memory chip. When the instrument in question was powered, the memory was powered from the main supply and a diode blocked current from flowing into the battery (lithium batteries are not meant to be charged). In this particular instrument, the diode had been installed backwards, so when the instrument was on the battery had energy fed into it. The resulting internal heating raised the internal pressure until the battery case let go.

Or maybe, in the GPS instance, the GPS receiver thought it could get a better assessment of its location if it was in lots of places at once.

⚡ Re: Karpov v. the Internet" game

Dick Mills <rj.mills@pti-us.com>

Sun, 1 Sep 1996 12:44:53 -0400

PGN wrote:

>Better yet, one grand master with others kibitzing by e-mail.
>If a grand master can play simultaneous matches, it should be
>no difficulty winnowing the e-mail suggestions in real-time.

I didn't see the smiley after your note Peter, think again.

[RISKS

TENDS TO SUPPRESS GRATUITOUS SMILEYS. HOWEVER, ONE WAS
EVIDENTLY

IMPLIED FOR THIS ENTIRE DISCUSSION, which intended to convey
that

the whole thing was rather silly. PGN]

Rather than an aid, this would be the ultimate sabotage for a
grand master
trying to concentrate on his game, while playing against a time
limit. It
would be akin to having many people trying to shout in his ear.

The same reasoning leads us to forbid citizens from using hand-
held radios
to kibitz the flying techniques of pilots while on final landing
approach at
the airport.

Dick Mills +1(518)395-5154

<http://www.pti-us.com>

AKA dmills@albany.net

<http://www.albany.net/~dmills>

✶ Re: Karpov v. the Internet" game

Pete Mellor <pm@csr.city.ac.uk>

Sat, 31 Aug 96 20:07:17 BST

PGN adds:-

> The result was clearly not a surprise. Only about 300 hundred
opponents?

Maybe that was the 300 people who did not realise that the
exercise was

farce!

> Suppose the group was
> composed of only a few grand masters? What would that do to
the odds?

Improve them for Karpov! (Each grand master would propose a
brilliant move
in each situation. These would generally be dissimilar, since
each grand
master would have a different vision of how the game would look
10 moves on.
Their brilliance would therefore be cancelled out.)

> Better yet, one grand master with others kibitzing by e-mail.

That is the point. Karpov was not (as far as I know - correct
me if
I'm wrong) playing the combined power of 300 brains.

Given 300 randomly selected players, most of whom would make
weak or
indifferent moves, the "most frequent" response chosen "by
computer" would
almost certainly be one of the weakest responses, and (as an
earlier
correspondent pointed out) not consistent with any single well-
thought out
plan of attack or defence. The group that Karpov was playing
were *not*
consulting one another to agree on the best strategy.

What is the point of having computer voting that looks one move
ahead
in opposition to a chess genius who thinks at least 7 moves
ahead?

It would be interesting to see an analysis of the resulting game.
I bet it was more crapov than Karpov!

Peter Mellor, Centre for Software Reliability, City University,
Northampton
Square, London EC1V 0HB, UK. Tel: +44 (171) 477-8422, p.

mellor@csr.city.ac.uk

✶ 19th Information Systems Security Conference

Jack Holleran <Holleran@DOCKMASTER.NCSC.MIL>

Sun, 1 Sep 96 08:28 EDT

ANNOUNCEMENT

19th National Information Systems Security Conference
Baltimore Convention Center
October 21-25, 1996

The full announcement [see below] is now available on-line and has

1. The final program (complete, long, & detailed)
2. Workshop and Demonstration information
3. Registration Form
4. Housing Form (Conference Hotel with pricing information)

Registration Information:

Tammie Grice, Conference Registrar
Voice: (301) 975 - 3883
FAX: (301) 948 - 2067
EMAIL: nissconference@dockmaster.ncsc.mil
WWW: <http://csrc.nist.gov/nissc/>

Cost: \$295, with early registration through September 19, 1996;
\$335 after September 19, 1996

✶ Information Security Conference - Cleveland

Robert Terry <utility@primenet.com>

2 Sep 1996 05:03:12 -0700

Second Annual NASA Lewis Research Center conference - "Perils of the

Internet and Practical Solutions - Confronting Threats from Hackers, Crackers, and Sniffers." 24-26 Sep 1996, Cleveland, OHIO.

For more Information: <http://www.dis.org/se7en/ndi>



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 18: Issue 41

Thursday 5 September 1996

Contents

- [China screens out Internet "Spiritual Pollution"](#)
[Edupage](#)
- [AOL curbs incoming spams](#)
[PGN](#)
- [AOL denial of service](#)
[Joe J. Birsá](#)
- [Warning on the use of GPS](#)
[Jim Easton](#)
- [More re: "More power to you"](#)
[Ralph Barone](#)
- [The unstoppable computer: PLURIBUS](#)
[Pete Kaiser](#)
- [Computers asked to identify suspicious baggage](#)
[Edupage](#)
- [Government database correlations](#)
[Bear Giles](#)
- [Hidden file info that you do not know about](#)
[Kirk McElhearn](#)
- [Windows 95 passwords](#)
[Bear Giles](#)

- [Re: Quadro tracker](#)
[Bear Giles](#)
 - [Accidental shooting down of F15 plane revisited](#)
[Chiaki Ishikawa](#)
 - [Re: Denial of service ... Netcom listservers](#)
[Greg Lindahl](#)
 - [Re: Back-country technology](#)
[Roger F Connolly](#)
 - [Re: FedEx monitoring of cellular...locations](#)
[Steve Holzworth](#)
[Gene M. Stover](#)
[Tony Lima](#)
 - [7th Computers, Freedom, and Privacy](#)
[Bruce R Koball](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✶ **China screens out Internet "Spiritual Pollution" (Edupage, 5 Sep 1996)**

Edupage Editors <educom@elanor.oit.unc.edu>

Thu, 5 Sep 1996 18:37:34 -0400 (EDT)

The Beijing government has begun blocking as many as 100 Internet sites that offer material the government deems unsuitable for its citizens -- including dissident viewpoints from Hong Kong and Taiwan, sites sponsored by U.S. major media organizations such as CNN and the Washington Post, and sexually explicit sites such as Playboy and Penthouse. An official described the blocked sites as suspected purveyors of "spiritual pollution." (*Wall Street Journal*, 5 Sep 1996, B12)

✶ AOL curbs incoming spams

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

Thu, 5 Sep 1996 8:40:38 PDT

Junk mail seems to be overwhelming all of us (including RISKS).
America

Online has decided to block completely all incoming e-mail from
five

Internet sites, three of which are run by Cyber Promotions,
Inc., in

Philadelphia. Those five sites apparently accounted daily for
about 700,000

pieces of unsolicited e-mail to AOL subscribers. Cyber
Promotions earlier

had sued AOL for interfering with its business, and also sought
an

injunction against AOL's blockade (although that injunction has
not yet been

acted on). Cyber also accused AOL of hypocrisy, because AOL
sends its own

commercial pitches to its subscribers. (CompuServe and Prodigy
have also

taken "comparable" steps.) [Source: Peter H. Lewis, item from
*The New York

Times* in *San Francisco Chronicle*, 5 Sep 1996, D3.]

Stay tuned for further developments in the commercialization of
the

Internet. Perhaps most frustrating is that would-be retaliatory
reverse

spammers often discover that the given e-mail FROM: address is
bogus, with

the spammer relying on a phone number instead.

✶ AOL denial of service

"Joe J. Birsa E-375B 8-284-5192" <birsaj@h01.pgh.wec.com>

Tue, 3 Sep 1996 16:18:02 -0400 (EDT)

Late last month, my sons complained that AOL wouldn't let them log on. When I called AOL, I found out that AOL suspended our service because the computer at the credit card company was unavailable and sent them a "try again later" message when they tried to debit my account. (I wonder how hard they REALLY tried to contact the credit card company.) Apparently because their computer couldn't talk to the credit card company's computer, the AOL computer decided to suspend my account and cut us off. Two days after this happened, I got a "snail mail" from AOL saying that I owed them money and my account was suspended until I contacted them. The amount involved was \$20.24.

The risks - If I was using my AOL e-mail for business purposes (or other serious use) I would have been cut off until I figured out that I needed to call them. I have no idea if (or how many) e-mail messages were "bounced" because of this. Again if this account was used for business, my reputation could have been seriously damaged because of this policy. Most companies that I am familiar with will not take such drastic action immediately if the normal payment process is delayed or interrupted.

BTW - The AOL representative I spoke to did not know if the AOL computer would retry until got an answer.

Joe Birsa

⚡ Warning on the use of GPS

Jim Easton <jeaston@johannsen.com>

Tue, 3 Sep 1996 20:54:42 -0700

Over the last few weeks I have experienced a series of GPS navigation errors ranging from minor (triggering RAIM) to as large as 20 miles horizontally and calculated GPS altitudes of below NEGATIVE 5000' MSL. I have never been given a NOTAM telling me to expect this performance.

Reading the current issue of AOPA Pilot, I now understand.

* First: Kudos to AOPA for finally telling us what is going on.

The military has been conducting GPS jamming exercises in Southern California affecting at least the Los Angeles and San Diego areas (that I have observed) lasting for times up to some 15 minutes (again that I have observed).

You should note that the vast majority of GPS units flying do NOT have RAIM and will NOT automatically flag an erroneous GPS position.

I would seriously warn pilots against trusting VFR GPS navigation in Southern California without cross-checks. Should a RAIM flag go on in an IFR GPS do NOT assume that because you are receiving lots of healthy satellites with good signal strength that you can ignore the warning. This is exactly what you will see when you are receiving jamming. Look at the calculated GPS altitude and calculated position error and cross check with any other

available navigation source.

Note that the government has decided to take down LORAN and VORs which will leave you dead when GPS is jammed. In spite of the absolutely predictable loss of airplanes and lives that this decision will cause, it is apparently cast in concrete. I believe that the plan may be to have a multibillion dollar fix to GPS after all alternative means of navigation have been shut down and a thousand or so people have been killed by GPS failure.

Jim Easton 4364 Bonita Rd., No. 166 Bonita, CA, 91902-1421
Tel: (619) 548-0138 FAX: (619) 470-8616

✈ More re: "More power to you" ([RISKS-18.32,40](#))

"Ralph Barone" <Ralph.Barone@BCHydro.bc.ca>
Wed, 04 Sep 1996 12:15:07 -0700

The following quote is from the Aug 19/96 issue of "Power Markets Week" (published by McGraw Hill). I thought you might find it interesting.

One Pacific Northwest market player stated that the new open-market, profit-making electricity industry is straining the existing Western distribution system. "This distribution system was never designed to maximize people's profits," he said. The price differentiation between the Northwest and Southeast trigger huge shifts in energy, which "can't be supported by the existing transportation system." he added.

Ralph Barone, Protection & Control Manager/HVDC Control Engineer
BC Hydro Ralph.Barone@bchydro.bc.ca

✶ The unstoppable computer: PLURIBUS

<kaiser@acm.org>

Wed, 04 Sep 1996 13:09:11 +0200

In my archives I came across this short article that Bernie Cosell wrote in August 1980. I'm posting it to RISKS, with his permission, because it seems worth getting the article into print -- it's still of interest -- and into all the archives where RISKS will be kept.

[Here's] a real world anecdote. It concerns the development of the software for the PLURIBUS multi-processor here at BBN. I think that the only details you need know about the PLURIBUS are that it is a symmetric multi-processor that uses (in essence) a network to connect together various buses; each bus contains only a limited amount of stuff: e.g., at most two processors, not all of common memory, only one end of a doubly interfaced I/O interface. Each processor has a small amount of local memory, but beyond that runs "through the switch" to execute code out of one of the common memories.

Since the hardware was designed to be extensible and resilient, the software was designed to be the same way. We were out there on the fringes figuring out how to build reliable, extensible, fault tolerant systems.

Without going into the details of how we made it all (mostly) work, let me describe some of the more amusing properties of the system. In particular, it was nearly impossible to stop the sucker once you got it going.

A pretty amusing circumstance crops up when someone would (innocently) wander up to the machine and push STOP on the console and mount a paper tape to load up some new software with. The console, however, only halts the processors on the bus it is on. Within a few seconds of halting the bus, the other (still running) processors in the system notice that some of their brethren have disappeared, and they reload them (lest their local memories had gotten clobbered) and then restart them. So as you stand in front of the paper tape reader, you notice that your "stopped" processor is happily back in the fold and you've been done in.

This actually happened (and caused something of a panic) when we shipped one to Washington. As the field engineer began uncrating the thing and powering back up and cabling the buses together, the shards of the IMP program we had last been debugging woke up and began sniffing about. By the time the whole machine was reassembled the software had long since found enough resources to make itself happy, and so had reinstated itself and was happily running along. He, of course, wanted to run some diagnostics, but couldn't (and never did) figure out how to get the system to go away and let him do his job:

Since the system is symmetric, both for software and hardware, there is really no critical component. If you unplug some of memory, the system will hiccup a moment, locate new copies of the code in the memory that is now gone and quietly continue running. Since the system always (if at all possible) maintains two copies of each software module and keeps them in separate memory modules, simply messing with memory won't stop the system. And on and on with plausible tricks that just wouldn't get the thing to die... (eventually, one of the software wizards in Cambridge was located and gave him the secret:

Plant an appropriate illegal instruction in common memory in a (carefully chosen) location which each processor would blunder across (and so stop) before either reloading any of the other stopped processors or noticing that the common memory checksum is clobbered and switching in a fresh copy.)

Even then you have to be careful, because if you happen to restart one of the processors before you load up your new code, it will quickly repair the damage to common and then seek out and restart its brethren and almost before you know it you're back where you started from... sigh....

The risks are pretty clear, aren't they?

Pete kaiser@acm.org +33 92.95.62.97, FAX +33 92.95.50.50

✶ Computers asked to identify suspicious baggage (Edupage, 3 Sep 1996)

Edupage Editors <educom@elanor.oit.unc.edu>

Wed, 4 Sep 1996 07:15:08 -0400 (EDT)

Officials working on an aviation commission headed by Vice President Gore and formed after the TWA Flight 800 crash are recommending that computerized background checks of passengers should be made to determine which customer luggage to search. Names, addresses, phone numbers, travel histories and billing records of passengers would be examined to look for irregularities that would suggest the possibility of terrorist activity. Civil libertarians are expected to object to the plan as an invasion of privacy.
(*The New York Times*, 1 Sep 1996, p17)

✶ Government database correlations

Bear Giles <bear@indra.com>

Thu, 5 Sep 1996 03:44:14 -0600 (MDT)

According to a sidenote on the minimum-wage bill recently passed, starting FY 98 (?) the federal government will maintain a list of all court ordered child support payments and all newly employed individuals, and then cross-correlate them. Needless to say, there appears to be no consideration of the inevitable problems with misidentification, security/privacy, etc.

Undoubtedly, "if you don't have children out of wedlock and

aren't divorced
you have nothing to worry about."

✶ Hidden file info that you do not know about

Kirk McElhearn <kirk@lenet.fr>
Thu, 5 Sep 1996 14:07:35 +0200

I work in France as a [bilateral] translator, and I am also a French editor for an American language learning software company. One of my roles is purchasing content, and negotiating rights.

I have recently been negotiating with a French TV station, to purchase some video. My contact sent me a draft contract as an e-mail attachment, but I had trouble opening it. When I opened it with a text editor, I discovered my contract, as well as 2 others.

It seems that they use Word. Now, my Mac is a Microsoft-Free zone, so I am not sure about how this works, but, if I understand correctly, you can save a document under Word which includes previous versions. (The doc I received was about 40k, and my contract was only 5 pages.)

This means that the person had been saving his contracts like that, and for a new contract, he just took an old one and made some changes. Well, the implications of this are obvious. I could have found, for example, that the price the previous client paid was far below what I had agreed to pay. Or there could have been other confidential information.

I explained this to my contact, who seemed a bit upset about not knowing what was in the file he sent me. I guess that many users of Word, and probably other WP software, may be in this situation also. If they were to read the manual...

Kirk McElhearn 91 rue de la Mesangerie 37540 St Cyr sur Loire
France
kirk@lenet.fr <http://www.nirvanet.fr/kirk/kirk.html>

[I think this problem has appeared previously in RISKS. PGN]

⚡ Windows 95 passwords

Bear Giles <bear@indra.com>
Thu, 5 Sep 1996 03:44:14 -0600 (MDT)

(This may be very old, but I just installed Windows 95.)

Windows 95 allows you to specify one password on the system... and changing the password on the Win95 screensaver does not require verification with any system-wide or user-specific passwords. This is a minor annoyance, but still an unnecessary one.

Bear Giles bear@indra.com

⚡ Re: Quadro tracker ([RISKS-18.22](#))

Bear Giles <bear@indra.com>
Thu, 5 Sep 1996 03:44:14 -0600 (MDT)

Archival update: the senior officers of the company which manufactured the "quadro tracker" were indicted on mail fraud charges. (AP, week or so ago; it was discussed previously in [RISKS-18.22](#))

✦ Accidental shooting down of F15 plane revisited ([RISKS-18.18](#))

Chiaki Ishikawa <ishikawa@personal-media.co.jp>
Fri, 6 Sep 1996 01:44:07 +0900 (JST)

I reported last year and early this year regarding the accidental shooting down of an F15 by a wing mate.

What happened: An F15 fighter plane of Japan's air force shot down another F15 during interception training over the Sea of Japan near the Honsyu island last November. Both planes were based in the Komatsu air base. One of the planes carried the live sidewinder missiles and despite the claimed safety mechanism, the missile was launched. The pilot of downed F15 parachuted down and was rescued.

Earlier reports I picked up suggested malfunction of safety mechanism such as static electricity problem of the master firearm system.

However, the investigation turned to a different direction, it seems. An article in the Asahi Shimbun on September 4th stated that the Komatsu military police of the Air force (my English translation of the unit name) filed formal charge with the local prosecutor's office against the 30 years

old pilot Jyun'ya Hino for disabling (turning off?) the safety mechanism and then pushing the missile launch button.

The charge mentioned is Kashitsu-Kokuh-Kiken-Zai. Kashitsu is a Japanese legal term for mistake, oversight, or an error. Kokuh here refers to air traffic. Kiken means danger. Zai is the legal word for crime. In a nutshell, the pilot is, if the prosecutor's office agrees, likely to be charged and tried with a grave oversight that brought about the serious accident.

My observation: It looks that the safety mechanism was overridden by human operator for whatever reason. This seems to be the conclusion of the air force investigation.

That military investigators filed charge with the prosecutor's office is a little puzzling, but I think the Japanese laws would require the handling outside the military court. I think petit crime such as stealing would be handled in the military. The military investigators must have found a serious neglect on the part of the pilot to justify the release of his name by filing formal papers to the prosecutor's office: the pilot's name had not been mentioned in the earlier reports at all (at least not in the newspaper articles that I saw in Asahi, Yomiuri, Nikkei newspapers).

If the military investigators are right, the accident was more likely to be the result of human error, and not that of computer-controlled system.

- * automatically reply to Precedence: bulk and Precedence: junk mail
- * ignore the Errors-to: header line [admittedly, I'm not sure if this "standard header" is in the RFC's]
- * repeatedly reply to the same From: line [cf. vacation(1)]

Writing correct mail handling programs is complex. Most PC vendors made and still make many mistakes when writing gateway programs. Good intentions are not a defense for sending thousands of unwanted pieces of mail.

Because of this problem, I do not have Reply-to: headers pointing back to any of my mailing lists -- this generally means only the author of the message sees the bounces. Then I get to deal with complaints like "why doesn't this list work like my other mailing lists?"

Sigh. Greg Lindahl D. E. Shaw & Co., L. P.

✶ Re: Back-country technology (Duane, [RISKS-18.40](#))

Roger F Connolly <james1_12@juno.com>

Thu, 5 Sep 1996 00:14:33 PST

This makes no sense to me. If they had known how to use the GPS receiver in the first place, they would have stored critical waypoints in it and wouldn't necessarily need a map to get back. Most modern handheld receivers will even point you in the right direction and show you a tracing of the path you've taken. However, if you stored no waypoints, and don't even know the approximate coordinates of where you want to be, a GPS receiver is about

as useful as something pretty useless.

✉ Re: FedEx monitoring of cellular...locations (Glassman, [RISKS-18.40](#))

Steve Holzworth <sch@unx.sas.com>

Wed, 4 Sep 1996 16:50:23 -0400

Cellular carriers are now required to supply 911 emergency service centers with caller locations to within some small distance (a block?). This is so EMS can locate people who call in via cellular. This can be thought of as an extension of ANI, used by such services already to determine your address immediately upon your calling into a 911 center.

Whenever your phone is on, it is communicating with the nearest cell(s) and flagging cell boundary crossings. This is necessary so that the cellular service knows which cell to use to contact your phone for inbound calls. In addition, individual cells can ramp your transmitter signal strength up or down to accommodate varying cell sizes.

>2. Is it possible for FedEx to capture information that Cellular One doesn't >know it's passing?

No. However, like ANI and CallerID, this is a capability that the cellular companies have apparently found a way to market, at least to customers that it might help, like FedEx. I imagine that the number you called was a "800" number or free cellular equivalent (*foo). Thus, FedEx

would argue
that they are paying for the call and deserve the additional
information...

✉ Re: FedEx monitoring of cellular...locations (Glassman, [RISKS-18.40](#))

"gene m. stover" <gangrene!gene@netcom.com>
Wed, 4 Sep 96 23:52:40 -0500

I have been a software engineer at various companies in the
cellular
industry for about two years. Since I am not an RF engineer,
what I say
about cell isn't authoritatively final, but short of that, it is
reliable.

There has been discussion of geographic mobile-location systems
for the
North American cellular system that do no rely on special
features like
adding GPS to the mobile. Such systems are:

1. Possible,
2. Of extremely limited accuracy (not nearly to the resolution
of a street
intersection; more like a 20- to 45-degree arc at least a mile
in radius),
3. Not implemented anywhere.

Even Cellular One didn't know your location when you made the
call, so FedEx
must have determined it some other way.

- > 2. Is it possible for FedEx to capture information that
- > Cellular One doesn't know it's passing?

No. (Well, since we're talking about a complex software system, a more accurate answer might be ``No more likely than the possibility that a C compiler would insert a backdoor when it compiled the Unix login program.''
;-)

gene m. stover (gene@CyberTiggyr.com)

⚡ re: FedEx monitoring of cellular...locations (Glassman, [RISKS-18.40](#))

Tony Lima <tony.lima@toadhall.com>
Wed, 04 Sep 1996 15:02:00 -0700

RO> Two days later, a FedEx operator confirmed that they are getting "new RO> systems" at some locations that are able to record the locations from which RO> cellular calls are placed.

What amazes me about this tale is that it's been widely reported in San Francisco area newspapers that the local 911 system can't tell where a cell phone call originates. It strikes me as perverse that FedEx can do something our local emergency system can't! Talk about your RISKS! - Tony Lima

Internet: tony.lima@toadhall.com (Tony Lima)

⚡ 7th Computers, Freedom, and Privacy

Bruce R Koball <bkoball>

Tue, 3 Sep 1996 12:37:14 -0700 (PDT)

THE SEVENTH CONFERENCE ON COMPUTERS, FREEDOM, AND PRIVACY
Call for Participation
San Francisco Airport Hyatt Regency Hotel
Burlingame, California
11-14 March 1997

CFP97: Commerce & Community will be sponsored by the Association for Computing Machinery SIGCOM and SIGSAC. The host institutions will be Stanford University and the University of California at Berkeley. Co-sponsors and cooperating organizations include the ACM SIGCAS, the Electronic Frontier Foundation, the Center for Democracy and Technology, the Electronic Privacy Information Center, and the WELL.

CFP97: Commerce & Community is the latest in a series of annual conferences assembling a diverse group of experts and advocates from the domains of technology, business, government, and academia to explore the evolution of information and communication technologies and public policy, and its effects on freedom and privacy in the United States and throughout the world.

Past CFP sessions have discussed, debated -- and often anticipated -- issues of great social import. In this tradition, CFP97: Commerce & Community will examine the social and policy questions posed by:

- * the growth of electronic communities;
- * electronic commerce and the commercialization of cyberspace;
- * the problems of legal and regulatory control of the Net;
- * the interests of privacy and property in the electronic domain;
- * high-tech law enforcement and security concerns.

The CFP97 Program Committee invites your suggestions for presentations on these or other important issues at the nexus of technology, business, public policy, freedom, and privacy.

Proposals may be for individual talks, panel discussions, debates, moot courts, moderated, interactive sessions or other formats. Each proposal should be accompanied by a one-page statement describing the topic and format. Descriptions of multi-person presentations should include a list of proposed participants and session chair. Proposals should be sent by e-mail to cfp97@cfp.org. If necessary, typewritten proposals may be sent to:
CFP'97, 2210 Sixth Street, Berkeley, CA 94710.

Please submit your proposal as soon as possible. The deadline for submissions is 1 October 1996. (Please note that we have extended our deadline for submissions)

For more information on the Computers, Freedom and Privacy Conferences, as well as up-to-date announcements on CFP'97, please visit our Web page at: <http://www.cfp.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 18: Issue 42

Tues 10 September 1996

Contents

- [Failure-mode risks revealed by Hurricane Fran](#)
[Dave Schulman](#)
- [Missile passes American Airlines Flight 1170 over Wallops Island](#)
[John Maddaus](#)
- [Re: Accidental shooting down of F15 plane revisited](#)
[Dick Mills](#)
- [Your BASIC electrocution -- "rats!", he said](#)
[Tim Steele](#)
- [Black-hole web forms](#)
[Prentiss Riddle](#)
- [RISK: Dangerous core dumps](#)
[Abigail](#)
- [Y2K - Yet another risk](#)
[John Elsbury](#)
- [Re: AOL curbs incoming spams](#)
[Brian Clapper](#)
[Bear Giles](#)
[Bear Giles](#)
- [Re: AOL denial of service](#)
[Peter M. Weiss](#)

- [Re: Netcom denial of service](#)
[Keith Moore](#)
 - [Re: Windows95 Passwords](#)
[Stewart Nolan](#)
 - [Microsoft VC++ property pages guaranteed to crash first time](#)
[Mark Mullin](#)
 - [1998 USENIX Security Conference, announcement/call for papers](#)
[Aviel Rubin](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ Failure-mode risks revealed by Hurricane Fran

Dave Schulman <capsalad@gate.net>

Mon, 9 Sep 1996 18:10:04 +0000

Having just survived a hellish weekend due to Hurricane Fran here in North Carolina, I found it interesting that several technological RISKS have only now come to light.

The area was clearly unprepared for a disaster of this magnitude, and is now paying the price for the "can't happen here" complacency apparent in the local utilities' failure to take preventive action which could have greatly reduced the suffering now happening here. Specifically, the electric utilities (and, by extension, their customers) have thus far resisted modernization in the form of buried power lines; presumably the rate increases necessary to finance this are anathema to existing customers. The lack of attention to trees growing close to power lines has now borne fruit, so to speak; about 100,000 subscribers have been without electricity for

over three days, as of this writing.

For what it's worth, I'm a recent transplant here myself, after having lived for nineteen years in South Florida, where hurricanes are an established fact of life and building codes are strict enough to persuade most designers to do the Right Things.

The Risks Forum has had much discussion in the past of the engineering of critical and safety systems, and how they should be designed to fail in a "safe" mode. It turns out that this design principle was lost on the people who designed the apartment complex in which I live. This complex contains electronic card-access locks with no manual overrides, and a "security" gate which fails into a "lockdown" mode. This is the sort of "safe" mode which might be appropriate for a prison, but certainly not for the only entrance/exit for a residential community. Had a fire broken out in the wake of the storm, I would very probably not be here to write this.

This complex is also provided with a so-called "security system" which is automatically hooked into each unit's telephone line. In the event of a power failure, these systems attempt to dial their monitoring stations to call for service. There is apparently no time-out interval for this; these alarms simply seized all affected phone lines and effectively kept them out of service until their backup batteries ran down after eight hours or so. This means, of course, that a power failure also guarantees loss of telephone service (for eight hours, anyway).

The RISKS here are all too depressingly obvious. It's a near-miracle that more people did not have to pay with their lives for such embarrassing lack of foresight.

Dave Schulman, Nortel, Inc., 400 Perimeter Park Drive,
Morrisville, NC 27560
Validation Engineer, Feature Test I (919) 905-4844; (919) 905-2549 (FAX)

✈ Missile passes American Airlines Flight 1170 over Wallops Island

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

Mon, 9 Sep 96 14:14:12 PDT

>Path: news2.digex.net!howland.erols.net!newsxfer2.itd.umich.edu!
uunet!in2.uu.net!news-in.tiac.net!news.gte.com!gte.com.gte.com!
jmaddaus
>From: jmaddaus@gte.com (John S. Maddaus)
>Newsgroups: rec.aviation.military
>Subject: Another missile/airline incident
>Date: Sun, 8 Sep 1996 14:33:04 GMT
>Organization: GTE Labs Inc
>Message-ID: <jmaddaus.10.3232D920@gte.com>
>NNTP-Posting-Host: 132.197.24.59
>Xref: news2.digex.net rec.aviation.military:106911

The **New Hampshire Sunday News** [8 Sep 1996] is reporting that at 1:45pm 29

Aug 1996 American Airlines flight 1170 was flying over Wallops Island,

Virginia, en route from San Juan to Boston when the captain reported

(apparently only to the company at the time) "a missile off the right wing".

The report has been confirmed by the NTSB, which has assigned an

investigator. Apparently, the FAA is investigating on its own as well. The paper goes on to mention the proximity to Wallops Flight Facility with nearby Navy installations at Norfolk and Lexington Park.

I'm assuming that normal cruise for the 757 would put it out of range of surface-to-air portables and there is no way to infer the trajectory based on what was said in the paper. However, note the headline "American Airlines Pilot Says Missile Zoomed by His 757", which is not what the quote above relates. [Not surprising. Headlines often have little to do with articles, because they are written by a headline specialist. John's subsequent comments, speculations, and questions have been omitted for RISKS. PGN]

John Maddaus

[Wallops Island has long been a rocket launching facility. Over 9 years ago, [RISKS-04.96](#) reported the case in which a lightning strike on the launch platform ignited three rockets and accidentally launched two of them. NASA had been intending to test launch capabilities in the presence of lightning storms. PGN]

✈ Re: Accidental shooting down of F15 plane revisited ([RISKS-18.41](#))

Dick Mills <dmills@albany.net>
Mon, 09 Sep 1996 00:31:49 -0400

Regular RISKS readers may remember several earlier articles about this incident that seemed to lay the blame on software bugs. Now, we hear a different story entirely and the cause is alleged to be something completely different. [Note that a single person, Chiaki Ishikawa, has simply reported the sequence as it arose. See [RISKS-17.65](#), -18.18, and -18.41. PGN]

There is a risk that occasional readers or researchers using search engines may come across the archived RISKS articles and use them to prove a point, or merely to sensationalize. They might never find the later articles that set the record straight. This is not a criticism of RISKS, but rather an attribute of any ongoing public discussion on the Internet.

There is also a new element to the risk. The resources needed to search massive amounts of news archives was, until recently, only affordable to wealthy organizations. Now we can all do it inexpensively, but most of us aren't trained investigators or journalists.

I believe that we should make airplane accidents a special case, and to voluntarily withhold public discussion and speculation until the accident report is in. Not forever, but until the reports are in and read.

There are several reasons why just airplane disasters are exceptional.

a) Early speculations about why the incident occurred are frequently wrong.

b) The actual report, issued after all the physical and other evidence has been examined, will be available within a reasonable time (months to one or two years.) There is ample opportunity to challenge the report's conclusion or offer other opinions after its release.

c) Speculations are often highly technical. This may lead non-technical people to ignore what is actually said as not understandable, and to look only at the headline and the source. RISKS is a respected source and some people may believe anything they read here is authoritative.

d) The sensational nature of air disasters makes the public and the media hungry for any tidbits. Technical debates intended for a closed audience aren't likely to stay closed for long.

e) Speculation may cause additional grief for the families of victims and crew or others involved. Reputations can be ruined. Even when the speculations prove true, the full report can include mitigating details that color one's judgement differently than partial information might.

Pilots in the hanger engage in gossip just like anybody else. When an air disaster occurs, you can bet the gossip flows freely. However, it is considered bad form to do so within earshot of laymen.

No doubt there are other risks that also deserve sensitive treatment, but to me airplane disasters stand out most clearly.

Dick Mills <http://www.albany.net/~dmills>

[It is intriguing that there are perhaps a dozen books on the KAL 007

case. It is not surprising that theories proliferate during times

that definitive reports are not available, but it is also not surprising

that, even with the presence of supposedly definitive reports, different

theories continue to propagate indefinitely. The TWA 800 case may become

another example. You may note that RISKS has been silent on that case,

eschewing speculation; however, there are some rather startling hypotheses

floating around. PGN]

⚡ Your BASIC electrocution -- "rats!", he said

Tim Steele <tjfs@tadpole.co.uk>

Tue, 10 Sep 1996 14:26:01 +0100 (BST)

The euthanasia-via-computer story in [RISKS-18.05](#) reminds me of an anecdote I

was told by a colleague in a previous job. He once worked for a pharmaceuticals firm and was required to find out if a particular candidate

molecule had any potential as an anti-anxiety drug. He rigged up a set of

cages for a number of rats, each of which could be warned (by a light, or

something) and shocked (by wires in the floor of the cage). The idea, as I

recall, was to warn the rats, then shock them briefly over a period of time

to see if the light alone subsequently caused the same amount of agitation.

If the drug was effective, it should make the rats less anxious (move around

less) when the light came on.

Unfortunately, the software he had written (in interpreted BASIC) had the undesirable feature that, if it stopped due to a runtime error, the output states [*] would remain as they were. During the night, the program hung during the "shock" routine, and when he came in the next day all the rats had been comprehensively electrocuted [*].

[* Rat-etat(s), especially if they were French rats? PGN]

⚡ Black-hole web forms

Prentiss Riddle <riddle@is.rice.edu>
Tue, 10 Sep 1996 10:09:11 -0500 (CDT)

This week I had the frustrating experience of trying to register for a conference using an online form that provided no feedback. I'll omit the name of the conference to protect the guilty. (The conference is web-related, so its organizers really should know better.)

The HTML form used the "mailto" action to deliver user input via e-mail rather than feeding it to a CGI program. Not only is "mailto" not supported by all web browsers, but it has the unfortunate feature of not providing any feedback to the user that the form has been submitted. In contrast, well-written CGI transaction handling programs will provide an acknowledgement screen and/or acknowledgement by e-mail (and very well-written ones may provide an encrypted electronic "receipt" as well).

The risks of online transactions that lack immediate feedback?

User

confusion and anxiety over whether the form was really submitted and the transaction really took place; redundant submission of forms as users re-submit in expectation of feedback; multiple transactions (e.g., multiple charges to the user's credit card) unless the back-end system has a bulletproof way to detect duplicate submissions; possible *non*-execution of transactions if the user's web browser really didn't catch the click on the "Submit" button and the user has been trained to expect no feedback; and wasted time and money as the user gives up on the online transaction and tries to straighten it out by telephone.

I do have some sympathy for small organizations trying to carry out transactions on the web without a prohibitive investment of resources. The marketplace for online commerce software is extremely chaotic right now, and do-it-yourself CGI programming is considerably more complex than learning to slap HTML tags into a document. But as the web moves from being a publishing system to being a more comprehensive system for commerce and other kinds of transactions, it is important that the people who set up online transaction systems recognize that their attention to reliability and user interface design must increase accordingly.

Prentiss Riddle riddle@rice.edu

⚡ RISK: Dangerous core dumps

Abigail <abigail@uk.fnx.com>
Fri, 06 Sep 1996 22:00:42 +0100

The following happened to me about a year ago:

Wanting to ftp a file to a remote server, I accidentally used a telnet client instead of an ftp client. Confused about the presented interface, I managed to type in some commands that crashed the ftp server on the remote site, dumping a core file.

A little later, I found the core file in my directory, and for no other reason than sheer boredom, I loaded it into a textfile. Removing all the control chars, I suddenly looked at a string that was all very familiar to me: my password.

It turned out the send password was stored in a variable which was allowed to live too long. (It got quickly fixed.)

I don't think I need to explain about the risks.

Abigail

[This is a very old risk, but worthy reiterating for younger readers. PGN]

⚡ Y2K - Yet another risk

John Elsbury <JELSBUR@clear.co.nz>
Tue, 10 Sep 1996 13:41:00 +1200

A British insurance company is reported to be providing a new insurance policy. They have been offering an "Alien Impregnation Policy", which is said to have sold 300 policies in a week: fired up by their success, they are now offering a "Virgin Birth" policy, on the grounds that a number of women are worried about the millennium. However, religious authorities are said to be cool towards the idea. (Since one of the larger organised religions depends on just such a manifestation of the Holy Spirit, this seems on the face of it inconsistent.)

This makes the Y2K computer-system date risks appear almost trivial.

The market may be limited however -- a straw poll of female colleagues indicated that this was the last thing on their minds at the moment.

[It will be interesting to see what evidence will be required for insurance claims on an Alien Impregnation Policy. I presume this will be a classic challenge for computerized DNA matching, and a glorious opportunity to become famous for the lab technician who first identifies alien DNA, or its equivalent! PGN]

✶ Re: AOL curbs incoming spams (PGN, [RISKS-18.41](#))

Brian Clapper <bmc@telebase.com>
Fri, 6 Sep 1996 15:32:57 -0400 (EDT)

According to today's on-line Philadelphia Inquirer

(see <http://www.phillynews.com/inquirer/96/Sep/06/business/AOL06.htm>)

U.S. District Court Judge Charles R. Weiner filed a temporary restraining order against AOL, ordering it to stop blocking junk e-mail sent by Cyber Promotions Inc. [The trial is scheduled for midNovember.]

Brian Clapper bmc@telebase.com <http://www.netaxs.com/~bmc/>

✶ Re: AOL curbs incoming spamming ([RISKS-18.41](#))

Bear Giles <bear@eris>

Sun, 8 Sep 1996 01:14:40 -0600

[...] Undoubtedly, the plaintiffs cited *Consolidated Edison v. Public Service Commission*, 447 US 530 (1980) in the injunction.

In the Supreme Court decision, the Court said that our right to be bothered does not justify limiting First Amendment rights. The solution is "[simple as] transferring [it] from envelope to wastebasket." [*Sex, Laws and Cyberspace*, 1996, pg 36]

The obvious counterpoint is that the US Postal Service is a "universal" service which is legally mandated to attempt delivery to all residents. With few exceptions (based on geography), receiving a letter requires no prior setup by the individual. Nor does the individual have to pay a monthly charge for access to his mailbox (in contrast to the *rental fee* for those boxes located in a post office). Nor does the individual have to sign contractual agreements with the postal service regarding

issues such as
"appropriate use" of the mail. (There are postal laws, but many
"appropriate use" restrictions are more restrictive.)

In contrast, online service providers require a "setup" before
they'll
accept e-mail for an individual. They charge for access to the
mail boxes.
And nearly all providers require users to agree to various
"conditions of
use" before the user can access his mail box.

These differences may not be enough to directly challenge the
court's
reasoning in the prior case, but it's enough to challenge the
assumption
that the matter has been definitively resolved. In 1980 the
USPS was the
sole mail delivery agent for the vast majority of Americans; it
was also
(until recently) literally a branch of the federal government.
Today we
have e-mail, fax/modems, FedEx, etc., all independent of direct
government
involvement.

As a wild-eyed extrapolation, this case may kill the attempts by
the USPS to
form its own e-mail service. If it's ultimately decided that
private ISPs
can block spammers while the USPS (as a quasi-government agency)
can't, few
people would choose the spammed version if they had an
alternative.

Bear Giles bear@indra.com

🔥 Re: AOL curbs incoming spamming (PGN, [RISKS-18.41](#))

<bear@indra.com>

Tue, 10 Sep 1996 02:56:04 -0600 (MDT)

>From what I gathered while scanning an article at lunch today, the spamming company had 1.5 million AOL e-mail addresses.

Assuming a typical message of 2k or so and a typical target of only 1% of the AOL subscriber base, the effects on AOL mailers could still be best described as "mail bombing." (15,000 messages totaling 30 MB).

Assuming the typical user has 2-3 messages in his inbox at any time, the total amount of disk space wasted on spams is 6-9 Giga_bytes, at best. In practice, with a distributed architecture the additional disk space (used or unused) required might easily total 20+ GB.

Another important factor to consider is the cost to backup an extra material in user's mailboxes.

The cost per AOL user is still modest, but why is it borne by AOL users, and not the party sending the unsolicited mail? (The sender of physical mail is always responsible for postage.) And what happens when it's not one company sending mail to 1.5 million subscribers, but a thousand direct marketers?

Bear Giles bear@indra.com

✉ re: AOL denial of service (Birsa, [RISKS-18.41](#))

"Peter M. Weiss +1 814 863 1843" <PMW1@PSUVM.PSU.EDU>

Tue, 10 Sep 96 08:36 EDT

Perhaps this subject is better thought of trying to make a silk purse out of a sow's ear? If you are going to put your reputation on (the) line via contracting with an Internet Service Provider, then it behooves you to have a service level agreement with them. Assuming that they are going to provide the service that you silently expect does not seem like a wise business decision to me.

Pete Weiss at Penn State

✉ Re: Netcom denial of service (Lindahl, [RISKS 18.41](#))

Keith Moore <moore@CS.UTK.EDU>
05 Sep 1996 22:08:38 -0400

Greg Lindahl <Greg-Lindahl@deshaw.com> writes about auto-responders that bounce messages with Precedence: {bulk,junk} and ignore the Errors-To header field, and admits that "writing correct mail handling programs is complex."

In fact, the situation is even more complex than that. Both fields are undefined, nonstandard, and can cause incorrect mail handling.

Use of the Precedence field varies widely. It was originally used by sendmail to determine queueing priority and more recently, to determine whether a nondelivery report returns the subject content. Some vacation

programs use it (among other heuristics) to determine whether to respond to a message. Some X.400 gateways use it to encode the X.400 Priority field, and return as nondeliverable any message that contains an unknown Precedence keyword. Some mailing list expanders use it as a means to prevent loops between peered lists, and therefore refuse to forward any message with certain Precedence values to the list membership.

As a result, there is no value for Precedence that is recognized by vacation, which does not result in mail delivery failure for some set of users.

Use of Errors-to violates a long-established (since 1980) standard which indicates where to send nondelivery reports. Within SMTP, they go to the MAIL FROM address, and mailing lists are required to set the MAIL FROM address to their list maintainer when distributing mail to the list membership. Outside of SMTP, nondelivery reports go to the address in the Return-Path field, which is set from MAIL FROM when the mail leaves the SMTP world. Some lists set Errors-to without setting the MAIL FROM address, some set only MAIL FROM, and some set both. MTAs that comply with the standards ignore Errors-to, but others use it to override MAIL FROM. Still others send nondelivery reports to both addresses, which in the worst case can cause a form of sorcerer's apprentice syndrome.

In fact neither field belongs in the message header while the message is "on the wire". Queueing priority and error return addresses are

both the concern of the message transport layer (e.g. SMTP), while the message header is intended only for use by the user agent. MTAs are supposed to ignore message headers, but instead they end up affecting whether a message gets delivered. And since these fields appear visibly in much list traffic, there is a widely held perception that they are correct protocol.

Plain-text protocols are easy to implement and debug, but they create the RISK that users will think they understand the protocol, and attempt to implement it without reading the specifications!

Keith Moore

<http://www.cs.utk.edu/~moore/>

[~moore/](http://www.cs.utk.edu/~moore/)

Computer Science Dept. / Univ of Tenn / 107 Ayres Hall /
Knoxville TN 37996

Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; OR ABRIDGING THE FREEDOM OF SPEECH, or of the press; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances.

- Amendment I, US Constitution (emphasis mine)

✉ Re: Windows95 Passwords (Giles, [RISKS-18.41](#))

"Stewart Nolan" <starsky@cqm.co.uk>

Tue, 10 Sep 1996 10:08:11 +0100

>Windows 95 allows you to specify one password on the system...
>and changing

>the password on the Win95 screensaver does not require

verification with
>any system-wide or user-specific passwords.

Having used this OS for about a year now, I find that it does not have a particularly secure setup.

If windows is waiting for a user login, there appear to be two ways around it:

1. Click OK.

When windows again prompts for the password, click cancel.

This seems to have the effect of logging the user in at the highest possible level if there are multiple users of the system, otherwise the user is logged in as the common user. From here it is simple enough to run regedit, causing all manner of havoc.

2. Press the windows key, or Ctrl-Esc if there isn't one.

This brings up task manager, again with the ability of running regedit from the command line.

The only way I have seen around this is to disable the login box (change the primary login to Windows), which will circumvent the appearance of the login dialogue. Unfortunately, this means there can be only one user, and if there is only one user, it isn't sensible to remove Registry editing tools.

Enable passwords at bios level, and switch it off when you leave your machine, for optimum security. Oh, and don't use win3.1x screen savers, they can be skipped by Ctrl Alt Del.

Stewart Nolan

⚡ Microsoft VC++ property pages guaranteed to crash first time

Mark Mullin <mullin@taligent.com>

Fri, 06 Sep 1996 13:57:06 -0700

Microsquish Stealth Bug Insertion Technology

While I'm kind of dismayed by the "if you can't innovate, litigate" philosophy so often applied to Microsoft, this is a particularly lethal little gem from their MFC team. In many development environments, this problem will almost certainly guarantee that your app will crash the first time it is executed on customer machines, but the crash will only happen once, and will mystify tech support.

The problem arises in the use of property pages, otherwise known as tabbed notebook dialogs, as they are designed and implemented in the Visual C++/MFC environment. VC allows the developer to use interactive resource editors to design the property pages, but IT ONLY DOES THE FINAL STEP OF THE PROCESS IN EXECUTING THE APPLICATION, not in the development cycle. This step, where the style of the page is changed in the resource will cause most machines to abort the software as it is attempting to change a read only resource.

What really concerns me from a risks perspective is that the traditional development model is to release an exe to the test/qa group, and then to ship this exe to production when it receives a blessing from

test/qa. This means that the exe shipped to production IS NOT THE SAME AS THE ONE THAT WAS TESTED, because the tested exe has been executed, and the one sent to production has not. Hence, every customer who launches the app for the first time will be rewarded with a crash, which can never be reproduced.

Yes, you can get around it with careful use of filtered exceptions. The problem is that this is rather insidious, and outside the realm of thinking of most developers, who view an exe as the final product of the development process. In this case, the final product is an executed exe.

Personally, I feel this is a lot like the Monty Python "Frog chocolates" sketch. VC too should have a great big warning sticker on it saying "An EXE from the linker is NOT A PRODUCT. YOU MUST EXECUTE IT TO MAKE A PRODUCT."

```
-- -- -- -- -- ORIGINAL MICROSOFT DOCUMENTATION -- -- --  
-- -- --  
Applies to class CPropertyPage, specifically the DoModal  
function that  
causes the page to be presented on the screen.  
  
virtual int DoModal( );  
  
[... standard usage documentation deleted...]  
[HERE IS THE INTERESTING BIT!!!]
```

Note. The first time a property page is created from its corresponding dialog resource, it may cause a first-chance exception. This is a result of the property page changing the style of the dialog resource to the required style prior to creating the page. Because resources are

generally read-only,
this causes an exception. The exception is handled by the
system, and a copy
of the modified resource is made automatically by the system. The
first-chance exception can thus be ignored. Since this
exception must be
handled by the operating system, do not wrap calls to
CPropertySheet::DoModal with a C++ try/catch block in which the
catch
handles all exceptions, for example, catch (...). This will
handle the
exception intended for the operating system, causing
unpredictable behavior.
Using C++ exception handling with specific exception types or
using
structured exception handling where the Access Violation
exception is passed
through to the operating system is safe, however.

🔥 1998 USENIX Security Conference, announcement/call for papers

Aviel Rubin <rubin@usenix.ORG>
Sun, 8 Sep 1996 07:54:12 -0700 (PDT)

7th USENIX Security Symposium
26-29 January 1998
Marriott Hotel-- San Antonio, Texas

Sponsored by the USENIX Association, the UNIX and Advanced
Computing Systems
Professional and Technical Association, in cooperation with: The
CERT
Coordination Center. Papers due: September 9, 1997. Program
Chair: Avi
Rubin, Bellcore

Conference home page: <<http://www.usenix.org/sec/sec98.html>>
Detailed guidelines for submission via e-mail to

<securityauthors@usenix.org>.

or telephone the USENIX Association office at (510) 528-8649.

USENIX Conference Office

22672 Lambert Street, Suite 613

Lake Forest, CA USA 92630

Phone: (714) 588-8649

Fax: (714) 588-9706

E-mail: <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 18: Issue 43

Weds 11 September 1996

Contents

- [IRS drops Internet tax filing plan](#)
[PGN](#)
- [RISKS of newspaper publishing](#)
[Rachelle Heller via Lance Hoffman](#)
[John Schwartz](#)
- [Safety of real-time systems \(PC versus SPS\)](#)
[Andreas Huennebeck](#)
- [Re: Accidental shutdown of F15 plane revisited](#)
[Robert Dorsett](#)
- [Lexis-Nexis personal information database](#)
[Larry Hunter from Privacy Forum](#)
- [Nebraska Automobile Title/Registration Records](#)
[Paul W Schleck](#)
- [Re: RISK: Dangerous core dumps](#)
[James Bonfield](#)
- [Re: Locating the position of cellular phones](#)
[Peter Campbell Smith](#)
- [Re: AOL curbs incoming spams](#)
[Fred K Herr](#)
- [AOL spamming case and direct e-mail in general](#)

[Lance J. Hoffman](#)

● [Info on RISKS \(comp.risks\)](#)

✶ IRS drops Internet tax filing plan

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

Wed, 11 Sep 1996 11:42:11 PDT

The IRS has apparently pulled the plug on its plans for Cyberfile, an electronic system that would have enabled taxpayers to file their returns directly without going through third-party service providers. An earlier launch of Cyberfile for April 1996 was put on hold when the Government Accounting Office identified some security weaknesses. The decision to abandon the project was evidently made in July. A GAO report just released blamed mismanagement and shoddy contracting practices. It also noted that the central computer was located in a dusty subbasement of the Agriculture Department subject to flooding, the computer-room doors had locks installed backwards (to keep the bad guys in?), and sprinkler pipes were too low. The report also observed that use of the World Wide Web (rather than toll-free direct dialups) represented security problems for taxpayers and for the IRS alike. At a 10 Sep 1996 hearing of the Senate Governmental Affairs Committee considering the Tax Systems Modernization effort more broadly, Senator Ted Stevens said, "It's an absolute fiasco." [Source: a *Los Angeles Times* article in the *San Francisco Chronicle*, 11 Sep 1996, p.A3]

⚡ RISKS of newspaper publishing

"Lance J. Hoffman" <hoffman@seas.gwu.edu>

Tue, 10 Sep 1996 19:20:36 -0400 (EDT)

> Date: Tue, 10 Sep 1996 17:14:19 -0400 (EDT)
> From: Rachelle Heller <sheller@seas.gwu.edu>
> Subject: What do you know about the WP Sunday break-in?
> To: hoffman@seas.gwu.edu (Lance J. Hoffman)
>
> Matt tells me that the Style section for Sunday's WP had a
break-in and
> someone changed the masthead prior to publication and it was
published
> without anyone's knowing it. [...]

Yep, I have it in front of me, freshly rescued from the recycle
bag. The
Sunday Style Section of *The Washington Post* for 8 Sep 1996 has
in its
masthead at the upper right corner of page F1:

"Published for You by a Large, Uncaring, Conglomerate".

Lance Hoffman

⚡ RISKS of newspaper publishing

schwartzj <schwartzj@twp.com>

Tue, 10 Sep 1996 19:33:23 -0400 (EDT)

The Sunday Style editor, Gene Weingarten, does this every week.
It is a
deeply subversive act, but it comes from within.

Weingarten is a deeply twisted man, and a treasure.

Sorry if this disappoints you.

A few favorite previous "ears," as they are called:

- * Mitnick was here
- * 25 Years of Error-Free Journalism
- * It's Not Very Good This Week
- * As Unbiased As the Next Pinko Rag
- * The Only Thing In This Newspaper That is On The Far Right
- * One was printed upside down and it said, "Hey, Why Am I on the Bottom?"
- * Another one printed upside down said, "Number One in Quality Control."
- * Another personal favorite: "Nice Bathrobe."

In fact, 90-95 percent of them are submitted by readers as part of the ongoing Style Invitational, the *Post*'s weekly, off-color humor competition. The Ear author is thanked in the fine print. It's a great thing -- a big corporation that (at least in one corner of one page one day a week) laughs at itself.

John Schwartz, speaking only for myself here at *The Washington Post*.

✶ Safety of real-time systems (PC versus SPS)

Andreas Huennebeck <ah@bruker.de>

Fri, 6 Sep 1996 14:12:48 +0200 (MESZ)

In the German newspaper "Elektronik" no. 18/1996 from 3 Sep 1996, intended for professional electronics hardware and software developers, appeared an article containing the views of several companies regarding the usage of PCs

(personal computers) running Windows NT versus SPS (Speicher-Programmierbare Steuerung = programmable control unit) for real-time applications. One of the views from the CEO of a company selling PC-based systems said (I translate and make shortcuts):

"Regarding the poor safety of a system running under Windows, my point of view is that every system has limited safety. Even the praised SPS will eventually cease to work - maybe not as soon as a PC, but sometime or other there is an end. But in most application cases the safety of a PC based system is high enough."

I think this is a strange kind of safety judgement.

Andreas Huennebeck Bruker Analytische Messtechnik GmbH
ah@bruker.de

⚡ Re: Accidental shutdown of F15 plane revisited (Mills, [RISKS-18.42](#))

Robert Dorsett <rdd@netcom.com>

Wed, 11 Sep 1996 14:04:06 GMT

> There are several reasons why just airplane disasters are exceptional.

All good reasons. However, one also has to deal with the political dynamics of a crash, both good and bad. The fact is, public safety can be affected by the results of a crash investigation. Therefore, to coin an old phrase, "the public has a right to know."

Even premature information can be accurate, and even, if misleading or wrong, can have unintended beneficial effects by putting pressure on both manufacturers and investigators to address specific public concerns.

Examples:

- The early grounding and microscopic probing after the American Airlines DC-10 crash at ORD in 1979 resulted in everyone in the industry becoming very familiar with the technical issues at hand. I doubt if anyone will ever use a forklift to mount an engine ever again.

- The author of Unheeded Warning notes his concerns (as a pilot) of the safety of the ATR-72 in icing conditions long prior to the eventual October 1994 crash. His book notes explicit steps taken to keep the issue alive in the media and thereby bringing political pressure to bear on the NTSB and FAA to maintain appropriate perspective in both the investigation and regulation of the aircraft. This pressure arguably resulted in FAA mandates to adjust the design of the anti-ice system on the airplane. Similar pressure was absent after a similar crash in 1988 in the Italian Alps.

- Each A320 crash ignites intense discussions on software reliability. No A320 has crashed as a result of a flight control system failure, but even incorrect speculation helps educate budding and practicing software engineers and discussion of the pros and cons of this implementation, which reflected the state of the art at the time, will hopefully help

encourage a sense of pragmatism when it comes to installing and developing safety-critical systems. In addition, since everyone has a personal computer these days, and therefore considers themselves experts, USENET discussions also have the effect of educating the lay public. An educated public is the enemy of political and corporate opportunists everywhere.

- I think we can all agree that the microscopic examination of ValuJet will have the eventual effect of making it the safest airline in the air, even though the scrutiny is politically motivated and arguably very unfair when compared to the operational reality of other airlines. That is, ValuJet will be safe if the airline isn't driven out of business.

- The NTSB frequently holds open hearings on major crashes. In at least one situation recently (in regards to the UAL 737 crash at Colorado Springs) they invited public comment. It's difficult for even the technical public (in this industry, several million people in and affiliated with the field) to comment if they aren't provided with "premature" factual information.

Lastly, let's keep in mind that the TWA crash, which I suspect may have helped shape your comments, is kind of exceptional. It crashed over the media capital of the United States, and likely of the world. Individuals coordinating the "victims' families" press conferences involved members associated with "victims rights" movements in other contexts, thus imparting some of their special skills and thus helping influence the

political
dynamics of this crash (compare family coverage of this crash
with any other
in recent memory). This extraordinary combination actually
resulted in
officials stating that the crash/crime investigation would be
put on hold
until bodies were all recovered. In the mean time, public
safety was
potentially compromised as physical evidence was lost: nobody
knows
whether a bomber might be running around. In addition, since
terrorism
seems very likely, the crash provides a longer-term interest
than is typical
for our usual mass-media reporting, which is designed for a 45-
second
attention span.

It's a political world, not a technical one. Unfortunately, the
real risk
comes from a cultural propensity to encourage the ignorant to
speak loudly
and assertively. That does not mean basic data should be
restricted, only
that those who glibly assert expertise from fluff seen on the
nightly news
should be shushed.

Robert Dorsett rdd@netcom.com Moderator, sci.aeronautics.
simulation
aero-simulation@wilbur.pr.erau.edu [ftp://wilbur.pr.erau.edu/pub/
av](ftp://wilbur.pr.erau.edu/pub/av)

✶ Lexis-Nexis personal information database (PRIVACY Forum Digest 05 17)

PRIVACY Forum <privacy@vortex.com>
Tue, 3 Sep 96 12:01 PDT

[PRIVACY Forum Digest Tuesday, 3 September 1996 Volume 05 :
Issue 17]

Date: Tue, 3 Sep 1996 11:22:15 -0400 (EDT)
>From: Larry Hunter <hunter@intr.net>
Subject: Lexis-Nexis personal information database

Lexis-Nexis sells a commercial database called "Ptrax" which holds detailed personal information on nearly all Americans (L-N claims it contains 300 million names). This database includes name, current address, up to two previous addresses, phone number, birth-date, social security number, mother's maiden name and possible other personal information. This database is kept quite current. Through the Nexis Express service, this information could be available to any individual with a credit card.

As most readers will be aware, such information could easily be used for theft of identity and other frauds. It is possible to have one's name removed from this database by making a telephone request. Call (800)543-6862, select option 4 ("all other questions") and tell the representative answering that you wish to remove your name from the Ptrax database. You may also send a fax to (513)865-7360, or physical mail to LEXIS-NEXIS / P.O. Box 933 / Dayton, Ohio 45401-0933. Sending physical mail to confirm your name has been removed is always a good idea.

As word of the existence of this database has spread on the net, Lexis-Nexis has been inundated with calls, and has set up a special set of operators to handle the volume. In addition, Andrew Bleh (rhymes with "Play") is a manager responsible for this product, and is the person to whom

complaints

about the service could be directed. He can be reached at the above 800

number, selection option 4 and then ask for extension 3385.

The information in this note has been been confirmed by me, and was

originally provided in forwarded messages from Russell Whitaker, Jason

Werner, Vern Winters, Katherine Florman and Reuben Snipper.

Larry Hunter hunter@intr.net

[For info on Lauren Weinstein's PRIVACY Forum Digest, see risks.info or risksinfo.html, or <http://www.vortex.com> . PGN]

✶ Nebraska Automobile Title/Registration Records

"Paul W Schleck KD3FU" <pschleck@oasis.novia.net>

Fri, 6 Sep 1996 15:09:57 -0500 (CDT)

Here in Nebraska, automobile titles and registrations are handled at the county courthouse level by the county clerk's and treasurer's offices.

Residing in the city of Bellevue, I received a renewal notice for a car of mine that I've owned for a number of years (I bought it for cash, so I've always had clear title). Strange thing was, the postcard had already been returned by the post office as undeliverable, finally reaching me after being resent. The name and address on it was:

Sarpy County
(my address)

This was curious, but I didn't think much of it at the time.

Near the end of the month, I went down to the Sarpy County courthouse in Papillion, paperwork in hand, expecting this to be a routine renewal. The clerk at the renewal counter noted amusingly that my name had been changed to "Sarpy County." She apologized for this, saying that they had recently gone to a statewide system and a lot of records were in error. She then noticed that the title number of my last year's registration card did not match the title number on my renewal notice. Attempting to look up my records on-line found that I was not listed as the owner of this car, Sarpy County was. The date of the new title was February of 1993. She called someone at the state and after a brief phone conversation, turned to me and asked:

"Was this an abandoned vehicle?"

Uh-oh. Everything suddenly clicked in my mind. My car was never abandoned, but I did leave it parked on a city street during snow removal in January of 1993. Though the street was not a snow emergency route, there is apparently a rarely-enforced ordinance that cars parked on public streets must be moved every 24 hours. Mine hadn't been moved in at least a week (it's an operational vehicle, I just don't drive it every day), and the small collection of snow around it made this obvious. I realized it had been towed after noticing it missing the same evening after I got home. After promptly retrieving the vehicle from the impound lot the next day, I received a letter in the mail from the Sarpy County Sheriff's office

indicating that the car had been towed and that I had 5 days to claim the vehicle before forfeiting it to the county. Concerned, I called the Sheriff's office and was assured that as long as I had reclaimed the vehicle such that the county was not in possession of it anymore, I had nothing to worry about (Physical possession of the vehicle struck me as an obvious sanity check against incorrectly initiating title claim proceedings against non-abandoned vehicles. For some unexplained reason, this sanity check was not performed). Operating under this assurance, and easily able to re-register and (re-insure) my car in 1993, 1994, and 1995, I was happily oblivious to the fact that the county claimed my title in error almost 4 years ago. I only became aware of this now, in August of 1996, at the registration renewal counter after the state finally synchronized its records.

Armed with this information, I was referred to the title counter, and then the Sheriff's office, the upshot being was that I had to ask the Sheriff's office to title the vehicle back to me. Fortunately, they were willing to do so without any hassles or significant delays. I signed their "Duplicate" title as "purchaser" and the Sheriff's office wrote out a \$10 check to the county treasurer (avoiding the insult that would have been added to injury if I had actually had to pay the title fee as a result of their mistake). I now hold an "Original" Nebraska title on my vehicle, once again. With this new title safe in my hands, and following good legal advice

regarding the risks of having duplicate, and contradictory, "original" legal documents lying around, I turned my original "Original" title over to be destroyed.

Identifiable Risky Behaviors:

- There seems to be at least a partial lack of obvious human sanity checks in the procedures for taking possession of abandoned vehicles. One would be whether or not the county is actually *in possession* of the vehicle. A corollary to this is, having decided they did own the vehicle, that the county did not seem to do a reasonable amount of tracking (and auditing after the fact) regarding the disposition of (alleged) county property, leaving the status of this vehicle indeterminate for years. One has to wonder if the same oversight would have happened if the title said "1996 Mercedes."

- Keeping records in at least two different places, and subjecting them to inconsistent, and rare updates, is just begging for trouble. I'm not sure how long the county and state records were out of whack, but I do know that I was able to get registration renewals in 1993, 1994, and 1995, even though the state records indicated that I was not the owner of the vehicle during that time. This suggests that at least part of the records have gone unsynchronized for years.

- The implicit data flow in old the system was correct in principle (propagate updates from the county level to a central

clearinghouse, i.e.

the state, then propagating those changes back downward to the county), and

the move to a new, single, integrated statewide system was an appropriate

one. However, the apparent inconsistency of, and long delays between,

record updates in the old system created the absurd situation where the

government agencies in buildings less than a few hundred feet apart (the

Sarpy County Sheriff's office, which took possession of the vehicle, and the

Sarpy County Courthouse, which tracked title and registration records) had

dramatically different versions of reality.

Risk Mitigations:

- Any sensible information system should save historical (i.e., "deleted")

records for auditing purposes. Having historical title records on-line made

it very easy for the employees at the title counter to quickly track down my

old title and determine its disposition (issuance of a new title to Sarpy

County). The date of the new title (early 1993) connected it in my mind to

the towing incident.

- The new system had an interesting (and perhaps unanticipated) soft failure

mode in that, even though the records showed that the car was not mine, I

still got a renewal notice which reminded me to go down to the courthouse.

I probably would have remembered anyway, but having a mismatch in title

number between my registration card and the renewal notice brought the error

to the attention of courthouse employees more quickly.

and, most importantly:

- Situations like these are often aggravated by customer service representatives who do not understand that computer-generated data can ever be in error, leaving the hapless customer to prove that it is incorrect.

Fortunately, the human employees at the Sarpy County Courthouse and Sherrif's Office understood the limitations of their computer systems,

particularly in light of a move to a statewide system that introduced (or at

least brought to light) a lot of errors. Sarpy County Clerk Debra

Houghtling, Captain Dan Jackson of the Sarpy County Sheriff's Office, and

many others got personally involved in working out this problem and reaching

a solution within an hour (The car was retitled back to me at no expense,

and minimal effort, within a few days).

Epilogue:

Later discussions with Sarpy County Treasurer Rich James (both by me and by

a friend of mine with courthouse contacts) indicated that this is a known

problem with the new statewide system. Sometimes the error is with the

government (as in my case), sometimes the error is with the owner (as the

old system tracked driver's license, registration, and title information in

multiple places, and sometimes the motorist forgot to update all of them).

The new statewide system will at least catch these errors, and prevent new

ones from happening in the future. Though he noted that mine was a rare

case, he did acknowledge that it is possible that similar ones are lying

around in the records and won't be discovered until the motorist tries to re-register the vehicle.

Warning to Nebraska Residents:

The recent transition to a single, integrated statewide system for tracking automobile title and registration information has either introduced errors, or brought to light incorrect title actions and inconsistent updates that have been lying undiscovered at the state level for as much as several years. If the ownership of your vehicle is in *any* doubt (such as if it was towed like in my example), or you have changed your name or address and failed to notify all appropriate government agencies, check with your county courthouse. Any errors won't be brought to your attention until you try to renew your registration. My experiences in Sarpy County seem to indicate that they will acknowledge the error and promptly correct it with the issuance of a new title, if necessary (If it was the county's or state's fault, and you are politely assertive about it, it appears likely that the agency responsible will pay any fees involved in correcting the records). Your registration can't be renewed until this new title is received, so go down early in your renewal month to avoid possible interruption in your vehicle registration.

Paul W. Schleck pschleck@novia.net <http://www.novia.net/~pschleck/>

⚡ Re: RISK: Dangerous core dumps (Abigail, [RISKS-18.42](#))

James Bonfield <jkb@mrc-lmb.cam.ac.uk>

Wed, 11 Sep 1996 09:53:08 +0100 (BST)

If the core file is in a users own directory then it's almost certain that telnet crashed, not the server (ftpd). As such a telnet core is likely to contain buffers of recently typed actions including your password.

It is perhaps preferable for core files to be dumped with mode 600. I don't know of any systems that will do this without also changing umask for all your other files.

On a related topic, really crashing the ftpd can also be dangerous. On our Solaris 2.5 box connecting via telnet and simply typing 'pasv' causes a core dump to be dumped to the remote systems root directory. This has two effects - it overwrites any existing core even on systems where you have no login (or root) access. Secondly it uses more disk space which may have implications for system logs if they're not on a separate file system.

James Bonfield, Medical Research Council - Laboratory of Molecular Biology,
Hills Road, Cambridge, CB2 2QH, England. 01223 402499 jkb@mrc-lmb.cam.ac.uk

⚡ Re: Locating the position of cellular phones (Stover, [RISKS-18.41](#))

Peter Campbell Smith <campbellp@logica.com>

Mon, 09 Sep 96 17:41:31 GMT

There is an interesting article in Traffic Technology International, Aug/Sept 96 issue about a system called CAPITAL that uses cellular phone calls as a probe to monitor road traffic around Washington DC. It describes an experiment which has been running for two years and which has demonstrated that this is an extremely cost-effective alternative to conventional means of traffic monitoring.

The system is independent of the cellular phone system per se, but has antennae on the cellular phone masts which listen to the cellular frequencies. Every time a call is initiated, CAPITAL locates the caller by a combination of directional multi-element antennae and time-of-arrival analysis between different masts. The geographical accuracy is reported to be to about 115m, and subsequent tracking allows the speed of the vehicle to be established within 30 to 50sec to an accuracy of 5mi/h.

At any time only less than 5% of vehicles are making calls, but this is a sufficient sample for analysing the traffic speed (though not presumably the traffic density). Moreover, when the traffic slows down even more people make calls, so there is a better density of data from the areas most interesting to those monitoring traffic flows.

It is claimed that the boxes ignore the voice content of the call and that the data they deliver has randomly assigned identifiers for each call, so that

nothing leaves the system which would allow calls to be associated with specific phones.

Peter Campbell Smith, Logica, London, UK campbellp@logica.com

🔥 Re: AOL curbs incoming spams ([RISKS-18.41](#) et al.)

"Herr, Fred K TR" <FKH1@trpo6.tr.unisys.com>

Wed, 11 Sep 96 10:39:00 EDT

The judge's injunction to prevent AOL from interfering with the subject spams seemed to rest on a comparison of free speech expressed via the USPS as against free speech expressed via on line message services, with the assumption, pending at least until the trial in November, that there is no essential difference.

There is, of course, a significant economic difference - which may have no relevance in discussing the constitutional issues - but which highlights a risk of computer and network technology to itself and its users. The risk is that the rapid reduction in costs and rapid growth in capability changes the economic balance so quickly that the system's stability, even survival, is dependent on the good manners (or common sense) of its user community until the entire system evolves to a new state of economic equilibrium.

Free speech via the USPS is anything but free, in the financial sense. The junk mail that I so readily send to the trash-to-steam plant

without opening
has at least four real financial costs associated with it. A
payment to the
postal service to deliver it. Payment to a printer to produce
it and
deliver it to the postal service. Payment to a mailing list
provider so it
can be sent to a real address. And payment of the costs related
to creating
the content (text and graphics). Thus the sender spends a few
dozen cents
to a few dollars to irritate me for a second and generate an
ounce of steam.

The spam advertiser, on the other hand, may have to bear some
creative
expense, but the other three costs are practically zero (divide
a modest
network access fee by a few million messages).

The paper mailer has to carefully balance the costs of "free
speech" against
the profit expected to result, and he is using a resource that
is in
equilibrium, more or less balancing the postal rates against the
people and
tools needed to handle a predictable volume of paper. The
spammer has no
concern for balancing cost against profit - the potential profit
of each
additional message delivered is always greater than the minuscule
incremental cost of the additional message. But the risk to the
delivery
system becomes quite large as the load rapidly exceeds the
service capacity
that assumed good manners would be the norm.

To restore equilibrium perhaps the delivery system could learn
to recognize
spams. When it does, it could credit the account of each
receiving mailbox
with a few cents, and debit the sender's account a similar
amount. If

spammers can still figure out how to make a profit in this new environment,
well at least the rest of us will pay less for access, and we may even make
a profit if we receive enough junk mail.

Oops! That will tip the equilibrium the other way as individuals start
getting multiple mailboxes in hopes of attracting lots of junk e-mail.

Fred Herr fkh1@trpo6.tr.unisys.com

✶ AOL spamming case and direct e-mail in general

"Lance J. Hoffman" <hoffman@seas.gwu.edu>

Wed, 11 Sep 1996 07:19:13 -0400 (EDT)

For those who wish to see some of the key players in action, a videotape of
the following event is available for \$50 from GWTV (The George Washington
University TV station) (attn Paul Caffrey, GWTV, 801 22nd St NW,
Washington
DC 20052, 202 994-8233). While the discussion is now a year
old, the
passion of the players is captioned on tape (or the non-passion
in the case
of the computer-impaired lawyer from the DMA). It might be of
interest to
some RISKS readers. Those in the Washington area might consider
coming to
the seminar series this year (third Tuesdays of each month, info
at
<http://www.cpi.seas.gwu.edu/Activities/>)

Lance Hoffman

CONSUMER RIGHTS WITH DIRECT MARKETING ON AND OFF THE

INTERNET :

DOES JUNK (E-)MAIL REALLYLY BYTE?

Panel Discussion, 21 Nov 1995

Marc Rotenberg, Electronic Privacy Information Center

Ram Avrahami, Concerned Consumer

Sanford Wallace, Promo Enterprises

Robert Sherman, Direct Marketing Association



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 18: Issue 44

Thurs 12 September 1996

Contents

- [GAO criticizes White House database controls](#)
[PGN](#)
- [Galileo Glitch](#)
[Peter Ladkin](#)
- [Recent KAL 007 discussion](#)
[Peter Ladkin](#)
- [Keeping Your Mouth Open: re: F-15 shootdown](#)
[Peter Ladkin](#)
- [Removal from Lexis' Ptrax database](#)
[Betsy P](#)
- [Encryption's debate-chilling effect on universities?](#)
[Lance J. Hoffman](#)
- [Re: Hidden file info that you do not know about](#)
[Edward Reid](#)
- [Fax machines that tell too much](#)
[Christopher J. Bell](#)
- [Unsolicited e-mail == unsolicited faxes ?](#)
[Edward N Kittlitz](#)
- ["Free Speech" == "Free Speech" ?](#)
[Barry Jaspán](#)

- [Re: AOL curbs incoming spams](#)
 - [Stanton McCandlish](#)
 - [David Allen](#)
 - [Dave Porter](#)
 - [Re: RISK: Dangerous core dumps](#)
 - [Matthew Hunt](#)
 - [Update 3 on GPS battery explosion](#)
 - [David Kennedy](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ **GAO criticizes White House database controls**

"Peter G. Neumann" <neumann@chiron.csl.sri.com>
Wed, 11 Sep 96 14:38:49 PDT

The White House maintains a database of some 20,000 people, and is used for sending greeting cards at Thanksgiving and Christmas, invitations to WH events, and other purposes. The GAO has criticized this database for its inadequate safeguards relating to access controls and lack of audit trails -- making usage monitoring very difficult. Apparently 150 White House employees have authorized access, although only 25 are regular users.
[Source: *San Francisco Chronicle*, p.A2, 11 Sep 1996]

[I presume the White House staff puts in a few bogus addresses so that they can tell when and how it is being used. I suppose they now also need to worry about a Dick Morris Worm attack.
PGN]

⚡ **Galileo Glitch**

Peter Ladkin <ladkin@TechFak.Uni-Bielefeld.DE>

Thu, 12 Sep 1996 16:27:31 +0200

In `Galileo team Wrestles To Keep Second Flyby', Aviation Week and Space Technology, 2 Sep 1996, p56, Michael A. Dornheim reports that `The Galileo orbiter went into "safe" mode on 24 Aug because of a computer error [...] Controllers began sending commands [to restore full operation] on 28 Aug, and the spacecraft and its computer were operating normally again on 29 Aug. [...] The error occurred in a CDS-A processor [...] some [...] data compression software had taken too long to execute, which shut all of CDS-A down. [...] Galileo then automatically entered the safe mode, which put CDS-B in charge and suspended all but basic engineering activities. [...] The cause of the error was not clear [at the time of reporting] [...] Galileo was resending a [Ganymede] image when the problem occurred [...] There are several pieces of data on the [...] recorder that have not been sent yet, and they will be overwritten by the second flyby.'

Peter Ladkin

✦ Recent KAL 007 discussion (Re: [RISKS-18.42](#))

Peter Ladkin <ladkin@TechFak.Uni-Bielefeld.DE>

Thu, 12 Sep 1996 16:24:11 +0200

Prompted by a query from a colleague, I searched for "KAL 007" on Altavista

<http://altavista.digital.com/>

to see what recent information had appeared on this major world incident.

In this note, I report sources and views of others and add some comments of

my own. I am not specifically endorsing any view or assertion here of *what

happened* during the incident or its aftermath.

Lt. Col. (retd.) Lester W. Grau, of the Foreign Military Studies Office, Ft. Leavenworth, KN, reviews a book on US-USSR relations from 1983-1990 by Don Oberndorfer, a diplomatic correspondent for the

WP from 1976, at

<http://leav-www.army.mil/fmso/books/reviews/turn.htm>

Grau says that `Izvestia conducted a further investigation of the KAL 007 aircraft downing [...] Mr. Oberndorfer apparently has not

read it since his book continues the Soviet myth about warning shots

being fired in front of the passenger plane.'

The Izvestia article has been translated by Roy F. Cochrun and is available as a zip file at

<http://www.clark.net/pub/royfc/zip/kal007.zip>

The translation as well as the Izvestia original is contained in a

number of files. (I got this URL from the last line of

<http://aeroweb.lucia.it/~agretch/RAFAQ/KAL007.html>

of which the main contents are a couple of messages from rec.aviation.military

that do not seem to contain definitive information.)

A short summary and endorsement of R.W.Johnson, Shootdown: Flight 007 and

the American Connection, Penguin, 1987, is at

<http://www.pir.org/books.87>

Johnson was a young politics Don at Magdalen College, Oxford (where I was in

the early 70's). He basically read all the NYT and WP reports concerning the

incident and aftermath to piece together a coherent story of who knew what

and when in the US executive after the shootdown. The

references alone form
an essential bibliography for political scholars. I was
impressed ten years
ago both by his method, and that there was a newspaper which
really did
contain so much useful information on a regular basis. But I
was so much
younger then.....

<http://www.iguide.com/books/reviews/brun.htm>

is a review by Jacob Levich of Incident at Sakhalin: The True
Mission of KAL
Flight 007, a recent book by Michel Brun (Four Walls Eight
Windows press).
Levich says Brun claims that KAL 007 was still airborne 46
minutes after the
'officially accepted' shutdown time, and crashed several
hundred miles to
the south of Sakhalin, not where it was reported to have
crashed. '[...] its
destruction was not the result of a single botched encounter
with Soviet
fighters, but part of a two-hour air battle in which at least
nine U.S.
military planes were shot down; the subsequent cover-up required
the covert
collaboration of at least four national governments.' Levich
thinks this is
'firmly grounded in reality' and 'accounts for more of the known
facts than
any "simple" explanation offered so far'. Based only on the
above quote,
one could really doubt it.

However, a much more sober and thorough review of Brun's book
appears at

[http://www.clarityconnect.com/webpages/bookpress/apr96/
chase.html](http://www.clarityconnect.com/webpages/bookpress/apr96/chase.html)

Edward R. Chase is former Editor-in-Chief of NYT Books and
senior editor at
Scribner, and was approached by Brun initially to see if there
was interest.
Chase introduced Brun to Richard Witkin, former NYT aviation
editor, and

David Pearson, author of KAL 007: The Cover-up. Chase, via Pearson, put Brun in touch with John Keppel, a retired Foreign Service officer, who collaborated with Brun. According to Chase, Brun's thesis was that KAL007 was a decoy posing as an innocent off-course flight, but was intending to cause the Soviet radars to light up. Such a thesis, I seem to remember, was proposed also by Pearson in a series of articles in The Nation and in his book. Brun's assertion of an air battle is new. Chase says: `Brun's book largely demolishes the U.S. propaganda line. Yet it is impossible for me to agree with all its conclusions. Although I respect his and John Keppel's intent, admire their industry, their skills, and their tenacity, I feel that their work could mislead the public by positing a conspiracy theory that is not credible in key particulars.'

Chase continues: `Brun's book makes very onerous reading for the layman. To follow his meticulous analysis of navigational and minute time discrepancies among the various transcripts and reports is a daunting task, rivaling in difficulty interpretations of texts by Kant or Derrida. However, his argument does demolish the official single-intrusion, single-deception, single-shutdown theory. [...] The two black boxes Yeltsin submitted as from KAL 007 in late 1992 and early 1993 are passing strange, apparently phonies, says Brun [...] Brun's proof of the falsity of these black boxes is one of the compelling sections of his argument. [...] the evidence Brun uses to demonstrate that [the] air battle occurred is all circumstantial,

painstakingly argued, but, for me and for experts I have queried, unconvincing to say the least. Nor do Brun and Keppel ever clarify the connection between the KAL 007 flight and the intrusion of U.S. military planes around the same time and place.

One wishes Brun and Keppel had confined their charge to the persuasive facts they elicit that there was a deliberate intrusion of breathtaking recklessness and stupidity that has been lied about ever since, and that the episode demands full, truthful disclosure.'

Chase also reviews: 'Another recent book, Warriors of Disinformation by Alvin A. Snyder, an excellent work highly praised by Mike Wallace and Marvin Kalb among others, powerfully supports Brun's charge of government lying in the KAL 007 disaster. [...] Snyder is the official who organised and presented the T.V. account of the shootdown of KAL 007 at the United Nations and then the world, using tape recordings of the Soviet fighter pilot's radio transmissions [...] What Snyder reveals is that the tapes were doctored. [...] Snyder reports that the full transcripts of the tapes show that, contrary to the U.S. allegations at the U.N., the Soviet pilot did fire warning shots, did circle 007 to get its attention, and tilted its wings to force the plane down, after being asked repeatedly by his ground controllers to do so. The Soviets never realised that the airliner was a commercial plane. [...] He also labels as a whopper the lie by U. N. Ambassador Jeanne Kirkpatrick that at no point did the [Soviet] pilots raise the question of the identity of the target aircraft. Snyder's

whole book is
first-rate, and his integrity comes across as unquestioned.'

Chase hopes that Brun's book will trigger Congressional
hearings, else we'll
have to wait until 2008, when the classified documents will be
disclosed.

I object to Chase lumping Derrida with Kant. But that of course
has nothing
to do with KAL 007.

In summary, Pearson and Brun seem to agree on the agent
provocateur
interpretation. Seymour Hersh's idea was an innocent INS
missetting in
Alaska (plus a lot of consequent coincidences), but I recall he
also
documented that parts of the USAF knew it had been an accident
when it
happened, contrasting unfavorably with what Kirkpatrick asserted
at the UN.
Johnson agrees with this, as far as I remember, and assembles
circumstantial
evidence that this was known at higher levels. Snyder confirms
this
interpretation. (I have not read the ICAO report, nor did I find
WWW info on
it.) Roll on 2008. Or write to your Congressperson. And let
us all hope
that nothing like this incident ever happens again.

Peter Ladkin

✶ Keeping Your Mouth Open: re: F-15 shootdown (Mills, [RISKS-18.42](#))

Peter Ladkin <ladkin@TechFak.Uni-Bielefeld.DE>

Thu, 12 Sep 1996 16:26:42 +0200

I sympathise with Dick Mills's ([RISKS-18.42](#)) desire to try to keep inaccurate information on airplane crashes out of the public domain. Robert Dorsett ([RISKS-18.43](#)) notes that public discussion is a given, and that even inaccurate discussion can be beneficial. To control disinformation, Mills proposes that people should keep silent until the final accident report is published. I don't see how that could help, and I do think it would hinder.

First, the NTSB itself does not follow that procedure. It issues documents at regular intervals. There are frequent press releases, and various information such as CVR transcripts is available before the docket is released. When the docket is complete, it is generally released to the public. This is usually many months before the final report appears. For example, the public docket for the AA965 accident near Buga, Colombia on 20 Dec 1995 was released on 16 Apr 1996. I quote: 'The enclosed material contains: factual reports only; no conclusions; no determinations of probable cause. Analysis of the accident will occur at a later date.'
(Punctuation mine).

Second, any NTSB information may be considered definitive, as may information from many other accident investigation boards. Such authorities do not 'speculate'. Valid conclusions may be drawn from this definitive information. A *valid* conclusion cannot be negated by further information, so there is little chance that this will contribute to spreading disinformation.

Third, the most common source of invalid conclusions is some sort of 'closed-world assumption' (as the logic programmers would call it). That is, assuming that the information one has is *all* the relevant information. For instance, knowing the AA965 pilots didn't know where they were and drawing the conclusion that that was the sole cause of the accident. That is, of course, mistaken reasoning. Better reasoning is to accept that this is one of probably many causal factors and expect others to be discovered. Discussion of the accident on that basis is not inappropriate.

At some point, a closed-world assumption must be made (we usually don't consider gremlins hammering bits off the wing as potential causes, pace The Twilight Zone). Such assumptions can be made explicit in any reasoning, as they should be in final accident reports. One should also not forget that much 'far-out' speculation bases itself on *not making* the closed-world assumption that others have made (most conspiracy theories, for example).

Fourth, 'peer review', that is, earnest discussion amongst interested people with various sorts of competence, including dissident opinions, is an accepted method of improving knowledge, both in academia and outside, in many societies. Consider it a psychological or social fact if you will, but it's a fact nonetheless.

Fifth, accident investigation boards are necessarily composed of a small number of the available experts in the field. I don't see any

reason why other competent should be enjoined to keep quiet if there are things to say. In particular, journalists are in general not technical experts and newspaper reports *will* appear that require discussion - and all too often, it seems, refutation. I don't see why, for example, a timely comment which includes such a refutation should wait until after an accident report.

Sixth, there are various interested parties (airplane manufacturers, airlines, pilot associations, air traffic control authorities, other government authorities) who have sensitivities that may conflict with a dispassionate explanation of the accident. Airlines must keep public confidence to continue in business. Pilots and air traffic controllers are sensitive to their statutory responsibility, and pilot unions may feel that they are thereby subject to disproportion blame. Regulatory agencies may be pressured by executive and regulatory branches of government, who can react precipitously to the public's precipitous reaction. Manufacturers are keen that the design and construction of their airplanes cannot be faulted. These alternative goals may skew views of accident causes. I should have thought that careful public discussion should be welcomed from those with some competence and no other goal than to try to clarify what happened.

Peter Ladkin

✂ Removal from Lexis' Ptrax database (Re: [RISKS-18.43](#))

<betsyp@vnet.net>

Wed, 11 Sep 1996 16:28:42 -0400 (EDT)

Spurred by [RISKS-18.43](#), I called Lexis's 800 number to request removal from the Ptrax database. I had to spend about 15 minutes on hold to do so; while I was on hold, a sweet-voiced recording assured me [PGN has inserted here the direct quote, provided by mwexler@Adobe.COM (Mike Wexler):]

The Ptrax database contains publically available information. It does not contain any private institution information such as credit card numbers, bank account information or mother's maiden names of individuals. You can not view social security numbers.

When I reached a human being and explained that I wanted to be removed, guess what was the only information he requested?

All those who said "Your Social Security number" get a prize. Whether or not the SSN is hidden, it seems to be a primary key as far as Lexis is concerned. The SSN is both necessary and sufficient; Lexis makes no attempt to verify that the person calling actually owns the Social Security number. The RISKS, alas, are obvious to everybody except our friends in the database business.

[REMARK: The SSN information is actually in the database; a given SSN can be used in queries, but SSNs allegedly cannot be retrieved. PGN]

[The 800-number message was reported and commented on variously by
mwexler@Adobe.COM (Mike Wexler),
adelano@frymulti.com (Art Delano)
(although Art was asked for his name, but not his full name!),
Jim Babka <babka@austin.ibm.com>.
PGN]

✶ Encryption's debate-chilling effect on universities?

"Lance J. Hoffman" <hoffman@seas.gwu.edu>
Tue, 10 Sep 1996 20:06:58 -0400

[Lance sent me a long copyrighted article that could be of possible interest to some of you. I omit all of the article.
PGN]

URL AND COPYRIGHT NOTICE FOR ORIGINAL ARTICLE:

Copyright (c) 1996 by The Chronicle of Higher Education, Inc.
<http://chronicle.com>

Title: Internet Users Irked by U.S. Restrictions on Encryption:

They think the rules compromise academic freedom and hinder efforts to combat on-line forgery

Author: David L. Wilson

Publication date: 13 Sep 1996

Source: The Chronicle of Higher Education

Section: Information Technology

Page: A27

✶ Re: Hidden file info that you do not know about (McElhearn, [R 18-41](#))

Edward Reid <edward@paleo.greensboro.fl.us>

Thu, 12 Sep 96 11:24:40 -0400

> ... you can save a document under Word which includes previous versions.

> [I think this problem has appeared previously in RISKS. PGN]

Several times I think ... but the misunderstanding persists.

When Word does a "normal" save with minor changes, it does not rewrite the entire document. Instead, it simply appends the changes and whatever information it requires to place them in the document. When working with large documents, especially on slower computers and disks, this makes an enormous difference in the time required to save a file -- a couple of seconds vs half a minute, for example. And since these same small computers adhere to the "save often or lose it" user-hostile paradigm, a faster save means fewer unhappy users.

The result is that interpreting a raw dump of a Word file can be quite difficult, and that many third-party programs that read other word processor files cannot read Word files unless you first do a "slow save". Also, deleted text may at times appear in the raw dump. This is mostly unpredictable, and does not consist of a "previous version" being included in the file.

Edward Reid

✉ Fax machines that tell too much

"Christopher J. Bell" <redriver@smart.net>

Thu, 12 Sep 1996 11:26:32 -0400 (EDT)

I was recently the recipient of a large number of faxes from potential job applicants. Many of the applicants were students and as such used university department fax machines where, presumably, they were required to use their own calling cards to make the long distance call.

In a number of cases, the originating fax machine had an automatic field displayed at the top of each page showing the number called. Presented to me quite clearly was a large number of calling card numbers with each user's PIN. Not only is this information displayed to the recipient, but the sender likely has no idea it's being made available.

Christopher J. Bell Pivot Computing cbell@pobox.com <http://pobox.com/~cbell/>

✶ Unsolicited e-mail == Unsolicited faxes ?

Edward N Kittlitz <kittlitz@world.std.com>

Thu, 12 Sep 1996 11:50:29 -0400 (EDT)

According to my rusty memory and 2 minutes of Altavista searching, there is a U.S. Telephone Consumer Protection Act of 1991 which requires: 1) identification of the sender at the top or bottom of the first transmitted page; 2) that unsolicited advertisements shall not be sent without invitation (which can implicitly be based upon the existence of a business

relationship).

If this Act is not unconstitutional, then it seems that the same type of law can be written regarding e-mail. The motivation is the same: 1) senders should be identified, not allowed to roam ISPs anonymously; 2) the receiver is paying for the cost of the advertisement, both in real terms (paper or message charges) and lost opportunity to receive desired items (out-of-paper, busy phone, mailbox size limits, time required to download junk e-mail which could have been spent looking for online smut or even online shopping at a competitor's web page).

✶ "Free Speech" == "Free Speech" ? (Herr, [RISKS-18.43](#))

"Barry Jaspán" <bjaspan@MIT.EDU>
Wed, 11 Sep 1996 18:08:58 -0400

After reading Fred Herr's statement,

>> The judge's injunction ... seemed to rest on a comparison of free speech
>> expressed via the USPS as against free speech expressed via on line
>> message services, with the assumption, ... that there is no essential
>> difference.

I had an interesting thought. Won't it be interesting if the US government (via its combined legislative and judicial authority) declares that "guarantee of free speech" applies to commercial advertisements at the cost of the unwilling recipient but does not apply to non-commercial

but

"indecent" communications among consenting adults?

Somehow, such an outcome does not seem even the slightest bit improbable to me; "inevitable" seems more like it. How depressing.

Barry Jaspán

✉ Re: AOL curbs incoming spams (Giles, [RISKS 18.42](#))

Stanton McCandlish <mech@eff.org>

Wed, 11 Sep 1996 13:03:41 -0700 (PDT)

None of that may ever come up. There is already a large pile of case law destroying the notion that First Amendment rights can be cost-shifted. No one owes you a printing press, you cannot send junkmail and expect it to be delivered postage due, and you can't junkfax people. Spamming cost-shifts most or all of the expense of advertising on the receiver. There's no First Amendment issue (other than AOL's right to exercise editorial control over a private service, something the TRO rather runs counter to.) I may not be an attorney, but AOL's case seems very strong. The First Amendment protects expression from interference by government, almost exclusively (there are exceptions, such as private schools having some limits on the censorship they may do of student publications, but these exceptions are very narrow, and are few and far between). AOL isn't the government, and their system is not a public space in the legal sense.

The philosophical question of whether AOL ought to have anything to do with restricting email in any way, even on their own service, is an important one - even AOL's internal forums have something of the character of a public, rather than a private, space - but such questions should probably be consciously and clearly separated from discussion of the legalities involved, which don't map very well to the theoretics.

Lastly, I think one should applaud AOL for shifting gears toward an individually-customizable filtration model. It's far better to have the choices in the hands of the end user, than in the hands of some intermediary, even if AOL offers some overridable defaults to filter out, like Cyber Promotions.

Stanton McCandlish, Electronic Frontier Foundation, Online Activist
mech@eff.org, <http://www.eff.org/~mech/>

✉ Re: AOL curbs incoming spams (Herr, [RISKS-18.43](#))

David Allen <dallen@nr.infi.net>
Thu, 12 Sep 1996 06:53:32 -0400 (EDT)

Fred Herr makes some very good points about the negligible costs of spam versus conventional junk mail, but I think the court erred in its comparison in a critical way when it cited First Amendment protection for spam. While advertisers (and common citizens) have a right to speak, **nobody** can compel us to PAY to listen. While the court would certainly find that

corporations
have a right to send junk mail or engage in telephone
solicitation, they
would rule quite differently if the corporations sent mail
postage due, or
tried to call us collect. The court would rule that we have
every right to
refuse to pay. Since on-line time costs money to the recipient
(no matter
how little), the comparison to regular junk mail is not
appropriate. More
appropriate is the FAX, where the owner of the FAX pays for the
paper.
Anti-Junk Fax laws were passed to stop "FAX-spamming" if you
will, and so
far have been found constitutional.

I think that legislation along the same lines would be
appropriate and
constitutional. Personally, I have a *major* problem with
corporations
being afforded constitutional protections as if they were
people, but that
is another debate entirely

David Allen , Contributing Editor, Internet Underground.
dallen@nr.infi.net
Columnist, Plan 9 from Cyberspace. See PCNet/MacNet, [http://www.
manziona.com](http://www.manziona.com)

🔥 Re: AOL curbs incoming spams ([RISKS-18.41](#) et al.)

dave porter <porter@cachelink.com>
Thu, 12 Sep 1996 13:18:43 -0400

This is a mind-numbingly trivial point, but I haven't actually
seen it
mentioned anywhere in print: if the spammers are so keen on
their "right" to

freedom of communication, why is it that the spam I receive seldom has a valid return address?

Maybe AOL should reject mail not "because it is spam" but "because it does not contain a valid return address" ?

[You should note that rejecting mail just because its return address is bad will lose some mail you really wanted. If RISKS rejected every piece of mail whose FROM: address is not a valid address, I would have fewer legitimate contributions to choose from. But many would-be subscribers get bounced immediately, because I remove their new-subscription address as soon as the acknowledgment bounces. As noted in [RISKS-18.39](#), I am looking forward to the new version of Brent Chapman's majordomo, which will do that automatically. PGN]

⚡ Re: RISK: Dangerous core dumps (Bonfield, [RISKS-18.43](#))

Matthew Hunt <mph@pobox.com>

12 Sep 1996 07:35:49 -0400

> I don't know of any systems that will do this without also changing umask
> for all your other files.

Linux does:

```
mph124:~$ uname -a
Linux mph124 2.0.18 #6 Sat Sep 7 12:49:09 EDT 1996 i486
mph124:~$ umask
022
```

```
mph124:~$ sleep 10 &
[1] 9679
mph124:~$ kill -11 9679
mph124:~$
[1]+  Segmentation fault          (core dumped) sleep 10
mph124:~$ ls -l core
-rw-----  1 hunt      users      278528 Sep 12 07:34 core
mph124:~$
```

🔥 Update 3 on GPS Battery Explosion

David Kennedy <76702.3557@CompuServe.COM>
12 Sep 96 02:35:59 EDT

```
>Extracted by Dave Kennedy [CISSP] National Computer Security
Assoc from
>C4I-Pro-Digest          Tuesday, September 10 1996          Volume
02 : Number 463
>Date: Tue, 10 Sep 96 09:39:00 +6
>From: Potter B MSgt ACC/SCXX <potterb@ns.langley.af.mil>
>Subject: c4i-pro Update to PLGR Battery Venting Event (Update
#3)
```

```
> Please pass to portable lightweight GPS receiver (PLGR)
users. Bottom
>line: Shorted diode (or NO diode due to wrong battery),
external power, and
>lithium battery can be a DEADLY combination. Short-circuit is
usual diode
>failure mode.
> Stay tuned. I'll pass-on updates as I receive them. Please
direct
>queries to Maj Lockhart, below. [MSgt Bob Potter]
>
> - - - - -
>
>From:      Lockhart, David E., Maj  CZU[SMTP:LockhaDE@gps1.laafb.
af.mil]
>Sent:     Monday, September 09, 1996 6:37 PM
>
>                                     9 September, 1996
```

> [...]

>Recommendation:

>

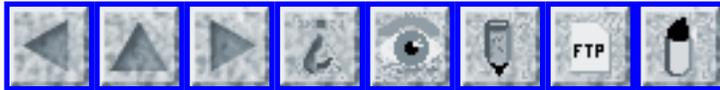
>When operating PLGRs on external power do not use lithium batteries in the prime power battery compartment.

>

>Develop a process that allows operators to use lithium batteries when

>operating in the stand-alone or internal power mode, but ensures the removal

>of lithium batteries prior to connecting to external power.



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 18: Issue 45

Friday the 13 Sep 1996

Contents

- [Cracker Attack Paralyzes PANIX](#)
[Edupage](#)
- [Re: PANIX SYN denial-of-service attack](#)
[Simona Nass](#)
- [100,000 DM offer to hack GSM phones](#)
[Klaus Brunnstein](#)
- [Linguistic RISKS](#)
[Aahz](#)
- [Civilian GPS navigation errors](#)
[Jim Easton](#)
- [Ariane 5 report in Aviation Week](#)
[Alan Frisbie](#)
- [Re: Accidental shutdown of F15 plane revisited](#)
[Dick Mills](#)
- [Re: Discussing aircraft accidents](#)
[Clive D.W. Feather](#)
[Mark Jackson](#)
- [Re: Windows 95 passwords](#)
[Jack Rochester](#)
- [Re: Passwords in files](#)

[James W. Birdsall](#)

● [Re: Fax machines that tell too much](#)

[Robert Sargent](#)

[Keiji Kanazawa](#)

● [Re: Unsolicited Unsolitude](#)

[Mark Eckenwiler](#)

● [Simple solution to AOL's legal woes](#)

[Andrew Marc Greene](#)

● [Sometimes junk e-mail is already a fax, legally speaking](#)

[Dan Franklin](#)

● [Re: Removal from Lexis' Ptrax database](#)

[Jim Walters](#)

● [Info on RISKS \(comp.risks\)](#)

✂ **Cracker Attack Paralyzes PANIX (Edupage, 12 Sep 1996)**

Edupage Editors <educom@elanor.oit.unc.edu>

Thu, 12 Sep 1996 17:18:14 -0400 (EDT)

Repeated attacks by a computer cracker have virtually shut down New York's Public Access Networks Corp., better known as Panix. The attacks have overwhelmed the computers' capacity to respond to requests for an ``electronic handshake'' by sending as many as 150 bogus requests a second.

``This is the first major attack of a kind that I believe to be the final Internet security problem,'' says a Lucent Technologies Internet security expert, who says he "has been waiting" for just such an event. Internet computers have no quick way of distinguishing these bogus requests from real ones, and even when security software is upgraded to ease the problem, the crackers could respond with even more intense assaults.

``There's going to

be the usual arms race,' ' predicts the Lucent security expert,
between
improved security measures and crackers' ability to disable
them. (*Wall
Street Journal*, 12 Sep 1996, B1)

[RISKS received various messages on this item, including from
Fernando Pereira <pereira@research.att.com>. PGN]

✉ Re: PANIX SYN denial-of-service attack

"Simona Nass" <sn@PANIX.COM>
Fri, 13 Sep 1996 11:10:37 -0400 (EDT)

The Washington Post [also] did an excellent story about it on
12 Sep 1996.
AP and others also picked it up. There's a statement on PANIX's
web page,
<http://www.panix.com>. We don't have the resources to answer a
lot of
technical questions right now because we've got our hands full,
but if
anyone who is familiar with the attack has ideas for possible
defenses, we
can be reached at staff@panix.com. -S.

Simona Nass staff@panix.com PANIX Public Access Internet

[At its heart, this is an unsolvable problem in general.
There are
some useful things you can do against very specific types of
attacks,
but there are too many types of attacks for a comprehensive
defense.
The best you can do in the near future might be to have some
early-detection capabilities to detect emerging attacks and
then
reconfigure dynamically accordingly. In the long run, it
might be

desirable to have more secure systems overall, which would require

(among other things) nontrivial authentication (i.e., NOT fixed passwords)

for any resource that might be abused. However, without draconian

measures, denials of service will always be possible, whether they

occur accidentally or intentionally. De RISKibus non disputandum est?

PGN]

✶ 100,000 DM offer to hack GSM phones

Klaus Brunnstein <brunnstein@rz.informatik.uni-hamburg.d400.de>

Fri, 13 Sep 1996 11:37:55 +0200

MobilCom, a subsidiary of German TeleKom (since 100 years monopolist onn

telephone communication in Germany, with its monopoly ending in 1998)

publicly offers 100,000 DM to a telephone hacker who is able to communicate

at the expense of the (national) number 0171-3289966. The related chipcard

is said to be safely stored in lawyer`s office. In an attempt to paint this

dubious offer somewhat "politically correct", the successful hacker will

have to donate his earnings to a social institution of his(her) choice.

Background of this offer is a recent magazine report informing the public

that German hackers know relevant details of the encryption algorithm (A5)

implemented in GSM mobile phones; this algorithm was always quoted to be

"secure" by GSM producers and service providers. According to the magazine`s

informant (a 22 year old male), he had informed German Telekom (provider of D1 mobile phone services) with details in May 1995. TV reports next week may "demonstrate" of how such knowledge may be used.

The story is "old vine in new bottles". Since GSM was specified in a joint European (essentially UK/French/German) exercise, material (though restricted to producers of GSM hardware and service personnel) were "available" in early 1990s, including the PSL code on which the encryption hardware is based. GSM methods implement an authentication process with which the caller`s chipcard-based key is compared with the database of applicable keys; after successful authentication, a session key is generated which is used by the encryption algorithm (A5) to "unbreakably" encrypt the communication. (Btw: for export to non-European countries, a weaker algorithm A5x is available; this approach is similar to NSAs policy of exporting US crypto methods :-)

"Security" of A5 and, more interestingly, A3/A8 (the algorithms for authentication and generation of session key) are "secure because they are not publicly known" (well-known principle of "Security by Obscurity"). This assumption was wrong as independent experts got copies of GSM algorithms (written in PSL) and could determine the effective length. Among others, Ross Anderson reported (on Internet) in 1994 about insecurity of A5 (he even published a C version of this algorithm which could have been used in determining weaknesses). In 1993, an expert group in a UK

university had easily cracked about 75% of the 114-bit key protecting communication.

GSM technology is used in 3 different German mobile phone services (D1, D2 and E-Plus) with more than 4,5 mio users. On the background of the media reports, users should look at details (when telephone with which number how long) more regularly, as falsification of individual chip cards may now become a new hacker sport, with the generous offer of Mobil Com.

Klaus Brunnstein (September Friday 13,1996)

⚡ Linguistic RISKS

Mean Green Dancing Machine <aahz@netcom.com>

Fri, 13 Sep 1996 06:16:36 -0700 (PDT)

I've recently been reading Donald Norman's latest book, *_Things That Make Us Smart_* (ISBN 0-201-62695-0 pbk). Instead of reviewing it, though, I'm going to illustrate how it has changed my thinking by criticizing a portion of an article I read last night in my partner's Wesleyan alumni magazine (Vol. LXXIX No. 1, Summer 1996).

"Which Way?" (author unclear) talks about the work of Scott Plous (Associate Professor of Psychology) and specifically his book *_The Psychology of Judgement and Decision-Making_* (McGraw-Hill, 1993). Here's a quote from the article:

Plous indicates how easily decision-making can go awry with an example drawn from a thirty-nine question survey at the beginning of his book:

"Linda is 31 years old, single, outspoken, and very bright. She majored in philosophy. As a student, she was deeply concerned with issues of discrimination and social justice, and also participated in antinuclear demonstrations."

"Which is more likely," he asks, "That Linda is a bank teller, or that

Linda is a bank teller and is active in the feminist movement?" Most

people guess that Linda is more likely to be a bank teller *and* a

feminist; that choice seems to be intuitively correct. Yet adding

detail to a scenario does not increase its likelihood. The more

general statement -- that Linda is a bank teller -- poses the fewest

restrictions and is the probable. Plous's point: Mathematical probability, not intuition, should guide this choice. To do otherwise

is to use a flawed decision-making process that increases the likelihood of error.

Before reading Norman's Things That Make Us Smart (TTMUS), I would

have simply nodded at the quote and continued reading. This time,

though, my immediate (almost experiential ;-) reaction was, "This is wrong!"

TTMUS contains a large section on the fallacy of confusing formal logic

with "logic of language". The six pages starting at 227 point this out

particularly clearly. In the quote above, much is made of Linda's

activism; when choosing an answer, "bank teller" is almost certainly

dismissed by most people as being irrelevant to the story --

this would
be made much clearer by asking whether Linda is more likely to
be a bank
teller or a computer programmer.

Which bring us back to RISKS: in user interface design, we must
be
careful which information we present to the user and how we
present it,
because the user will **not** interpret the information according
to the
rules of formal logic. I strongly recommend that everyone here
pick up
a copy of TTMUS; with any luck, it will change the way you
think, too.

Aahz (@netcom.com)

✶ Civilian GPS navigation errors

Jim Easton <jeaston@johannsen.com>

Thu, 12 Sep 1996 22:54:59 -0700

[Background:] I am a pilot who flies a small airplane equipped
with a GPS
satellite navigation system approved by the Federal Aviation
Administration
for use in clouds (IFR). I have been experiencing in flight
warnings that
the system has been (flagged) unusable somewhere around 1% of
the time it is
used. Lest you think this is trivial, you can consider driving a
car whose
windshield went opaque 1% of the time you were driving.

So far I have been told the following:

- 1) Some early GPS's were shipped with a defective Digital Signal
Processing
chip. This was corrected in later units.

2) Several different models have substantially similar computational algorithms.

3) When sufficient satellites are received, some units discard barometric altitude information for purposes of position calculations. A satellite declaring itself "healthy" is NEVER discarded automatically in these units.

Erroneous computed GPS altitude is a good warning indication of a bad position fix. Usually barometric altitude is more accurate than the altitude civilian GPS units compute from satellites (because of SA/AS).

4) US DOD mandates testing GPS units in its inventory against jamming. This testing has resulted in interference to civilian units to a radius of some 100 miles.

5) Commercial GPS satellite simulators are widely available.

6) Were one to hook up a GPS satellite simulator to an amplifier and antenna, one could disable many civilian GPS's at will. IFR certified units would give RAIM warnings, but would not give usable navigation information.

(RAIM is a consistency check of computed positions found generally only in IFR certified GPS units)

7) All GPS units lacking automatic satellite elimination capability are likely to be similarly vulnerable. Presently, automatic satellite elimination is mostly on GPS intended for sole means of navigation overwater.

8) VFR (not certified by the FAA for use in clouds) only GPS

units are not
required to indicate that their computed positions are erroneous.

9) Because GPS is extremely accurate almost all the time, many pilots have fallen into the habit of trusting GPS positions without cross checking against other means of navigation, or even against the computed errors displayable by the GPS unit itself.

I would greatly appreciate knowing of any errors in this information and/or additional information relevant to civilian GPS navigation use.

I think one can assume that a pilot getting a wrong position at night in the mountains, or no position in clouds in the mountains could have a problem.

Jim Easton 4364 Bonita Rd., No. 166 Bonita, CA, 91902-1421
Tel: (619) 548-0138 FAX: (619) 470-8616

✈ Ariane 5 report in Aviation Week

"Alan Frisbie" <frisbie@Flying-Disk.Com>

Fri, 13 Sep 96 09:05:47 PDT

The 9 Sep 1996 issue of *Aviation Week* contains the first section of the inquiry board's report on the Ariane 5 failure. The title is "Ariane 5 Report Details Software Design Errors", and is on pages 79-81.

I particularly liked the board's comment in the final paragraph: "The board is in favor of the opposite view, that software should be assumed to be faulty until applying the currently accepted best practice methods can

demonstrate that it is correct."

Alan E. Frisbie, Flying Disk Systems, Inc., 4759 Round Top Drive
Los Angeles, CA 90065 1-213-256-2575 Frisbie@Flying-Disk.
Com

✉ Re: Accidental shutdown of F15 plane revisited

Dick Mills <dmills@albany.net>

Thu, 12 Sep 1996 22:51:20 -0400

Mr. Dorsett, in [RISKS-18.43](#), and Mr. Ladkin, in [RISKS-18.44](#), disagree with my call for discretion in public speculation about airline disasters, in [RISKS 18.42](#).

Both argue that open and lively dissuasion of the issues can have real value. True, but neither man offers substantial reasons why such discussions aren't equally valuable if conducted more discretely. I also think their arguments also show single-mindedness in that airline safety and finding the correct conclusion are the only factors to consider.

Publicity about airline accidents makes people fear flying. Some fraction of those people will choose to drive to their destination, using a much more dangerous mode of transportation. Public discussions could increase airline safety but result in a net decline in total public safety. I can't prove that the net change is positive or negative, nor do I believe anyone else can prove it. Nevertheless, neglecting the secondary consequences of public debates is shallow.

I may also have overstated my call for discretion in my original message. I have no wish to stifle serious discussion among technically oriented interested parties. I merely object to it being done in such a public forum. Surely we can arrange more closed forums or e-mail list servers. Total secrecy and security aren't necessary, but a little more discretion is. If the NTSB is indiscreet, it too should be censured. It should not be interpreted as a signal that it is OK for us to be indiscreet too.

The Internet, Usenet in particular, is one of the most public forums ever invented. This is a particularly inappropriate place for sensitive subjects.

American daytime TV has been filled with talk programs that show people discussing the most sensitive and sensational subjects imaginable. The public seems to enjoy the voyeurism. I expect that nearly all of us detest this development. Is it surprising to realize that we may be unwittingly engaging in analogous activities?

Finally, I must take strong exception to one part of what Mr. Dorsett wrote:

- The author of _Unheeded Warning_ notes his concerns (as a pilot) of the safety of the ATR-72 in icing conditions long prior to the eventual October 1994 crash. His book notes explicit steps taken to keep the issue alive in the media and thereby bringing

political

pressure to bear on the NTSB and FAA to maintain appropriate perspective in both the investigation and regulation of the aircraft. This pressure arguably resulted in FAA mandates to adjust

the design of the anti-ice system on the airplane. Similar pressure

was absent after a similar crash in 1988 in the Italian Alps.

If the facts were as Mr. Dorsett states, I think this is deplorable. Just

think what it means to "keep the issue alive in the media and thereby

bringing political pressure to bear". This subjects questions of engineering safety to the same kind of handling as the O.J. Simpson trial.

It stirs up fear among the general public to give the issue emotional

strength and appeal. The word that describes precisely that set of

circumstances is demagoguery. Demagoguery is never praiseworthy.

(My apologies to non-native English speakers. I understand that demagoguery

is one of the least translatable words in the entire English language, but

in this case, it is the only word that fits.)

Mr. Dorsett expands on that theme when he says "It's a political world, not

a technical one." I say no, never. Mixing demagoguery and science is

irresponsible. It must never be tolerated.

Dick Mills <http://www.albany.net/~dmills>

✉ Re: Discussing aircraft accidents (Mills, [RISKS-18.41](#))

"Clive D.W. Feather" <clive@demon.net>

Fri, 13 Sep 1996 14:42:10 +0100 (BST)

> No doubt there are other risks that also deserve sensitive
> treatment, but to
> me airplane disasters stand out most clearly.

Funny, but I read that item, and it struck me that it applied
almost exactly
to railway accidents.

Clive D.W. Feather Associate Director, Demon Internet Ltd.

<clive@demon.net>

Director CityScape Internet Services Ltd. <cdwf@cityscape.co.uk>

+441813711138

[Well, when I read that item, it struck me that it applies
rather

broadly to almost everything that RISKS has tried to do for
the past

11+ years. Your humble and obedient *Designated Holist*, PGN]

✶ Re: Discussing aircraft accidents (Mills, [RISKS-18.41](#))

Mark Jackson <mjackson@wc.eso.mc.xerox.com>

Fri, 13 Sep 1996 05:14:48 PDT

As it happens, the *Columbia Journalism Review* web site is
currently

carrying a 1990 feature on the difficulties of reporting on
aircraft

accidents before all the facts are in. See

http://www.cjr.org/boot_reprint/boot.html

Mark Jackson - <http://www.alumni.caltech.edu/~mjackson>

⚡ Re: Windows 95 passwords ([RISKS 18.41](#))

Jack Rochester <jrochester@endor.com>

Sat, 07 Sep 1996 09:45:36 -0500

Bear Giles points out that Win95's handling of passwords is annoying. What's more, it points out the poor system design because there is no correlation between system, screen saver, or on-line login passwords. As has been pointed out by many, Win95 is an unsecure operating system.

I learned this in a most amusing way recently, when I was setting up my new Hitachi notebook computer. The first task was to install Windows 95 and select a password. After rebooting, I decided to see just how secure it was and typed the password incorrectly several times. Each was rejected, but then I clicked on "Cancel" in the dialog box and -- lo and behold! I was granted access.

Jack B. Rochester, Joshua Tree Communications, Cherry Hill Farm,
Cherry Hill
Road, Grafton, New Hampshire 03240 jrochester@endor.com 1-603
523 8350

[*Which Is Of Endor?* PGN]

⚡ Re: Passwords in files

"James W. Birdsall" <jwbirdsa@picarefy.picarefy.com>

Thu, 12 Sep 1996 14:32:23 -0700

[RISKS-18.42](#) and 18.43 discussed the possibility of passwords being found

in core files. While it is certainly a risk, there are mitigating factors: 1) a program has to crash at a time when it still has a password in memory, 2) an attacker must have access to the resulting core file, and 3) the attacker must inspect or copy the core file before the user (or possibly the system) gets rid of it.

A much worse risk, and one which is unbelievably still with us, is the storage of cleartext passwords in "password-protected" files. There is no need for a program to take an unusual action (crash) at a particular time, nor is there usually any time limit, since the resulting file is usually desired by the user and kept around for some time, if not permanently.

This risk was brought to mind recently when I had a need to break into a password-protected file that is part of a product made by the company I work for. The file is used to install certain macros in another company's product and the macros are password-protected to prevent accidental changes by end users. We (the development team) knew what the password was supposed to be, but it wasn't working. On an off-chance, I opened the file in a text editor and started scrolling through the mostly binary contents. Toward the end of the file, I found a string which matched the supposed password but differed in case, which both turned out to be the password and explained the problem. Bad enough that the password was stored in cleartext, but it caught my eye because it was preceded by the cleartext string "Password:"!

For us, this lack of security doesn't matter, since the password protection is intended only to discourage accidents and our support group will give the password to any user who needs it. Others may not be so lucky, and of course who knows what other currently-shipping products may suffer from the same risk?

--James

⚡ Re: Fax machines that tell too much (Bell, [RISKS-18.44](#))

Robert Sargent <RSargent@Cisco.COM>

Fri, 13 Sep 1996 10:40:24 -0400

This is a known bug in the older (3.4 ??) versions of Delrina's WinFAX.

Robert Sargent 423-671-0273 Pager: 800-365-4578 cisco
Systems, Inc.

⚡ Re: Fax machines that tell too much (Bell, [RISKS-18.44](#))

"Keiji Kanazawa" <keijik@microsoft.com>

Thu, 12 Sep 1996 16:12:27 -0700

Not only does the receiver see the credit card number, a lot of fax machines store those credit numbers as part of the record of what numbers were dialed when.

✉ Unsolicited Unsolitude (Re: [RISKS-18.44](#))

Mark Eckenwiler <eck@panix.com>

13 Sep 1996 11:32:38 -0400

>From: Edward N Kittlitz <kittlitz@world.std.com>
>According to my rusty memory and 2 minutes of Altavista
searching, ...

This is correct. See 47 USC 227(d) (requiring footprint) and 227
(b)
(barring unsolicited commercial faxes). [>...]

The federal appeals court in California, the Ninth Circuit,
upheld the
fax-ban provision of the TCPA in *_Destination Ventures_* (1995) on
precisely this cost-shifting rationale. For an article of mine
discussing TCPA (and concluding that while it does not now apply
to
junk e-mail, it could constitutionally be expanded to do so), see

<http://techweb.cmp.com/net/issues/036issue/036law.htm>

>From: David Allen <dallen@nr.infi.net>
>... I think the court erred in its comparison in a critical
>way when it cited First Amendment protection for spam.

I think it's crucial to point out that the court **did not** base
the TRO on
free speech law, contrary to the suggestion of some RISKS
readers. Even
Cyberpromo's lawyer has stated that their argument was based on
theories
like tortious interference with contract, and not on any
supposed First
Amendment right.

I agree that the TRO was improperly issued, but I think too much
has been
read into it. It's simply the judge's way of preserving the

status quo so
he doesn't have to think hard about the issues until trial.
(It's crucial
in this respect to remember that the TRO was issued in the
context of an
ongoing lawsuit between the parties.)

Mark Eckenwiler eck@panix.com

✂ Simple solution to AOL's legal woes

"Andrew Marc Greene" <amgreene@mit.edu>

Thu, 12 Sep 1996 15:55:06 -0400

Perhaps AOL should offer its users a special "spam-free" service. Certainly, if users request that AOL filter their incoming e-mail, then the purveyors of [ugly]-mail spams would have no leg[alism] to stand on.

- Andrew Greene

✂ Sometimes junk e-mail is already a fax, legally speaking

Dan Franklin <dan@copernicus.bbn.com>

Thu, 12 Sep 1996 19:46:42 -0400

I've been using the following legal information, which I picked up from another mailing list (Keith Bostic's /dev/null list), in my responses to junk e-mail these days. So far I haven't yet received junk e-mail on my home computer while it had a printer attached, but one of these days...

Under US Code Title 47, Sec.227(b)(1)(C):

"It shall be unlawful for any person within the United States to use any telephone facsimile machine, computer, or other device to send an unsolicited advertisement to a telephone facsimile machine"

A "telephone facsimile machine" is defined in Sec.227(a)(2)(B) as:

"equipment which has the capacity to transcribe text or images (or both) from an electronic signal received over a regular telephone line onto paper."

Under this definition, an e-mail account, modem, computer and printer together constitute a fax machine.

The rights of action are as follows. Under Sec.227(b)(3)(B):

"A person or entity may, if otherwise permitted by the laws or rules of court of a State, bring in an appropriate court of that State --

- (A) an action based on a violation of this subsection or the regulations prescribed under this subsection to enjoin such violation,
- (B) an action to recover for actual monetary loss from such a violation, or to receive \$500 in damages for each such violation, whichever is greater, or
- (C) both such actions. If the court finds that the defendant

willfully or knowingly violated this subsection or the regulations prescribed under this subsection, the court may, in its discretion, increase the amount of the award to an amount equal to not more than 3 times the amount available under subparagraph (B) of this paragraph."

For the full legal text USC Title 47, Section 227, see: <http://www.law.cornell.edu/uscode/47/227.html>

Dan Franklin dfranklin@bbn.com

✉ Re: Removal from Lexis' Ptrax database (Re: [RISKS-18.43](#) and 18.44)

Jim Walters <jwalters@spock.resd.honeywell.com>

Fri, 13 Sep 96 08:12:32 CDT

I was motivated (as I'm sure others were) by the [RISKS-18.43](#) blurb about Lexis-Nexis and their "legal community" serving database (the tiny quote is from their pleasant-sounding recording of the day). I first called in to their 800 line on the afternoon of 12 Aug, 96. I sat and listened to their recording for about half an hour while I was working on something else. I had to get up, so I decided to take the nice recording-lady up on her offer of leaving a message. When I tried, the voice mail system declared that the voice mailbox was full and no further messages were being taken. The nice recording-lady promptly hung up on me. I tried again this

morning (13 Aug 1996), and the recordings have all changed and are now instructing those concerned with removal of names from the database to make all requests "in writing". They give instructions to mail to their address (given in [RISKS-18.43](#)) or to fax them the request at (513) 865-1930 (different from [RISKS-18.43](#)). Just wanted to let people know that the procedure appears to have changed, due no doubt to the overwhelming responses they have most likely received.

Jim Walters jwalters@spock.resd.honeywell.com

["Kevin Johnsrude" <kevinj@roguewave.com> reported that he gave up after being on hold for half an hour, finally voicemailing (as requested) only his full name and address

--

before the voicemailbox overflowed with too many requests.

Peter.J.Scott@jpl.nasa.gov also noted the change to fax/snailmail. 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 18: Issue 46

Monday 16 September 1996

Contents

- [Maryland Lottery Computer Glitch](#)
[Scott Lucero](#)
- [Spider Minus Dog Equals Death](#)
[David Kennedy](#)
- [Virus pushes actress over the edge. No Backup?](#)
[Donald Mackie](#)
- [Minnesota disconnected from the world for 12 hours](#)
[Theodore M.P. Lee](#)
- [VeriSign's policy statement](#)
[Drew Dean](#)
- [Airliner interference from a COMPAQ mouse, revisited](#)
[Mark Brader](#)
- [Re: Accidental shutdown of F-15 plane revisited](#)
[Robert Dorsett](#)
- [AT&T -- Lessons forgotten](#)
[Bob Fieldhouse](#)
- [Word for Windows risks, continued](#)
[Jeremy J Epstein](#)
- [Re: Microsoft VC++ property pages guaranteed to crash first time](#)
[John Vert](#)

[Mark Mullin](#)

● [Re: Windows 95 passwords](#)

[Dirk Frankston](#)

● [Re: AOL curbs incoming spams](#)

[Bernard Peek](#)

● [More thoughts on junk mail](#)

[aahz](#)

● [Re: Sometimes junk e-mail is already a fax](#)

[Mark Eckenwiler](#)

● [Info on RISKS \(comp.risks\)](#)

⚡ **Maryland Lottery Computer Glitch**

lucero <lucero@optec.army.mil>

Fri, 13 Sep 96 18:18:36 EST

The Washington Post 13 Sep 1996 reports that a software error caused the wrong lottery numbers to be distributed to the state's 3,800 outlets. More than 22,000 people successfully bet on one or more of the numbers, but threw out their tickets thinking they lost. Others mistakenly thought they had won. Getting one or two numbers right gets people \$1-\$5, although two people bet numbers entitling them to \$5000 in this six-state lottery.

The firm, which recently won the contract to run Maryland's lottery games, stated that the numbers were correctly entered, but two of the six numbers were altered in the transmission process. A spokesman said, "To the best of our knowledge, it was a software error." The Post noted that the firm recently lost its contract in Arizona due to

computer problems.

Evidently, one of the RISKS is getting bad press.

Scott Lucero

🕷 Spider Minus Dog Equals Death

David Kennedy <76702.3557@CompuServe.COM>

13 Sep 96 20:28:18 EDT

Courtesy of Associated Press via CompuServe's Executive News Service:

Engineer Killed

>> HUNTINGTON BEACH, Calif. (AP, 13 Sep 1996) -- A spider may have
>>tripped a motion-sensitive alarm, and a police dog was out sick.
>>Authorities say the combination led to the accidental killing
>>of an elderly man.

>> On another night, a police dog instead of an officer with
>>pistol drawn would have searched the darkened manufacturing
>>business where 77-year-old Theodore E. Franks was shot and
>>killed Wednesday.

o Dogs normally check our burglar alarms, but police were down to one dog, and that dog was sick.

o Third alarm in seven months, second in 48 hours.

o Franks living inside the company so he could work during the hours he otherwise would have been commuting.

[DMK: Inverse telecommuting?]

o Police officer checking building found Franks unlocked room, entered, was startled by Franks and accidentally shot him in the leg. Shot him in the femoral artery. Franks died of exsanguination before he could reach the hospital.

>> "After hearing the facts, I think it's pretty obvious this >>was an accident," Wayne Franks said after visiting the office >>where his father was shot.

>> [Alarm Company] checked the alarm system Thursday, >>telling company owner [name deleted] a spider probably set it off, >>The Orange County Register reported Friday.

>> "I feel bad. It was my alarm," [name} said. "That damn spider."

Dave Kennedy [CISSP] Research Team Chief, National Computer Security Assoc.

⚡ Virus pushes actress over the edge. (No Backup?)

Donald <donald@iconz.co.nz>
Mon, 16 Sep 96 20:00:27 +1200

According to an interview with Margot Kidder in People Online, a computer virus was the last straw leading to her nervous breakdown.

The virus (not identified) on her computer destroyed files, including the book she had been working for three years. Having, apparently, no backup copies, the entire work was lost. This loss triggered her widely reported nervous breakdown.

Must go and back up this message before I post it....

Donald Mackie FANZCA FRCA, Middlemore Hospital, Private Bag
93311, Otahuhu,
Auckland, New Zealand ph +64 9 276 0000 dmackie@middlemore.co.
nz

✶ Minnesota disconnected from the world for 12 hours

Theodore M.P. Lee <tmplee@MR.Net>

Sun, 15 Sep 1996 20:38:03 -0500

The primary network that serves Minnesota (the Minnesota Regional Network) was cut off from the Internet for 12 hours today [15 Sep 1996]. (My understanding is that **all** major nets and systems, private and public, in Minnesota ultimately get their connection to the rest of the world through MR.Net.) Following are the initial announcement that they had discovered they had been cut off and the final announcement indicating service had been restored:

```
> Date: Sun, 15 Sep 1996 10:35:22 -0500 (CDT)
> To: all@MR.Net
> Subject: NET-DOWN: MRNet isolated from rest of Internet...
>
> Greetings,
>
> MRNet has become isolated from the rest of the Internet. The
T3 line to
> InternetMCI is up, but we are not receiving the routing
table. We have no
> details on what happened, or the extent of the problem.
InternetMCI is
> working on the problem, currently they do not have an
estimated time to
```

> repair. According to MRNet's network monitoring we have been
isolated
> since about quarter to 6 this morning (Sunday).

> Date: Sun, 15 Sep 1996 19:28:36 -0500 (CDT)
> To: all@MR.Net
> Subject: NET-UP: Routing restored from MCI
>
> Greetings,
>
> MCI routing was restored at 19:15 today. Downtime was over 12
hours.
> MRNet will be checking routing tables to see that we are
getting most of
> the routes we should, and will be spot checking networks to
make sure that
> our routing announcements are getting out.
>
> There has been no official word from InternetMCI as to the
specific cause of
> this outage, or why it took more than 12 hours to fix. MRNet
will be
> following up with InternetMCI to get an explanation on Monday.

FURTHER MESSAGE FROM TED:

Date: Mon, 16 Sep 1996 16:53:53 -0500
>From: tamplee@MR.Net (Theodore M.P. Lee)
Subject: Minnesota Cut Off From the World For 12 Hours!

This morning's paper [16 Sep 1996] here in Minneapolis had a bit
more on it
-- the head of MR.Net said he had heard of problems as far away
as Seattle
and Atlanta. I was out all day and if there has been an
explanation MR.Net
hasn't sent it out. Probably no point to adding this to the
RISKS item
until an explanation is forthcoming.

>Yesterday, the Downers Grove node of CICNet (much of the Big
10, plus
>Notre Dame, the University of Chicago, and other schools) was

also cut

>off from the outside world by InternetMCI... perhaps it was a related outage.

>

>John R. Grout Center for Supercomputing R & D j-
grout@uiuc.edu

>Coordinated Science Laboratory University of Illinois at
Urbana-Champaign

🔥 VeriSign's policy statement

Drew Dean <ddean@CS.Princeton.EDU>

Fri, 13 Sep 1996 15:16:11 -0400

I was looking at VeriSign's web page, in particular their Certification Practice Statement (CPS). <URL:<https://www.verisign.com/repository/CPS>>

Buried among the legal gobblygook, I found the following:

"the certificate is being used exclusively for authorized and legal purposes, consistent with this CPS," from Section 7.2.(v), Representations by Subscriber Upon Acceptance,

and

"By accepting a certificate, the subscriber assumes a duty to retain control of the subscriber's private key, to use a trustworthy system, and to take reasonable precautions to prevent its loss, disclosure, modification, or unauthorized use." from Section 7.3, Subscriber Duty to Prevent Private Key Disclosure.

I do not understand what Section 7.2 is supposed to mean.

Authorized by
whom? Legal according to which country's laws? Section 7.3's
requirement "to
use a trustworthy system" would seem to eliminate about 99.5% of
the market:
almost all computers are not trustworthy, even if they are (in
practice)
trusted.

RISKS: Although you agree to all of this (and that you've read
it) before
you receive your VeriSign certificate, it is not reasonable to
expect people
to wade through a 13-chapter work.

If almost nobody meets the requirements for using VeriSign, what
good is it?
Who accepts the risk of something going wrong, when the
conditions for use
are not met, and VeriSign issued a certificate knowing that
these conditions
are not met? A false sense of security can be worse than no
security....

Drew Dean

✶ Airliner interference from a COMPAQ mouse, revisited

Mark Brader <msb@sq.com>
Sun, 15 Sep 96 00:11:10 EDT

Newsgroups: sci.aeronautics.airliners
Path: sq!fastlane.ca!n3tor.istar!tor.istar!east.istar!news.nstn.
ca!newsflash.concordia.ca!newsfeed.pitt.edu!news.duq.edu!
newsgate.duke.edu!agate!news.Stanford.EDU!unixhub!ditka!bounce-
back
>From: Dewayne Matthews <dewayne@wiche.edu>
Subject: Re: Can't use GPS on Alaska Airlines
References: <4vkuns\$54b@news1.ni.net> <321E425F.70C0@macromedia.

com> <321F5320.CC0@mail.wwd.net> <airliners.1996.1750@ohare.Chicago.COM> <airliners.1996.1778@ohare.Chicago.COM>
Organization: University of Colorado at Boulder
Date: 13 Sep 96 03:03:33

In article <airliners.1996.1750@ohare.Chicago.COM>,
> Dave Benjamin <dbenj@slip.net> wrote:
>It seems incomprehensible that aircraft avionics that MUST frequently
>fly over high-powered radio transmitters could be so susceptible to stray
>onboard RF. My understanding is that the restrictions on in-flight use
>of electronic devices is based entirely on unsubstantiated anecdotal
>evidence.

Well, here's some anecdotal evidence. About 3 years ago, I was in seat 1D on a Delta MD88 flying at cruise altitude over NE New Mexico on a clear summer afternoon. A flight attendant came out of the cockpit (flightdeck?) and with a clear sense of urgency made a PA announcement to turn off all portable electronic devices and instructed the other FAs to check all the passengers. They quickly reported that the only device in use was a laptop in seat 2C (right behind me) and this guy was having trouble saving his file so he hadn't turned it off yet. The first FA said "I'm sorry sir, but you have to turn it off NOW!" He did. She went back into the cockpit, and came out about two minutes later. She went over to the guy in 2B, apologized, and said that when the captain called her into the cockpit the first time (this is an exact quote) "All the gauges were black." (The MD88 has a "glass" cockpit.) She said that they were just now coming back on. She then said (I'm not

making this up) "The captain wants to know if you have a Compaq computer."

He said, with surprise, "Why, yes, it IS a Compaq." It was a older one with an external mouse. I told them that I had read somewhere that external mice greatly exacerbated the problem. I then had another cup of coffee.

It made a true believer out of me.

Dewayne Matthews

✶ Re: Accidental shutdown of F-15 plane revisited (Mills, [RISKS-18.45](#))

Robert Dorsett <rdd@netcom.com>

Fri, 13 Sep 1996 18:52:03 GMT

Dick Mills <dmills@albany.net> writes:

> Mr. Dorsett expands on that theme when he says "It's a political world, not a technical one." I say no, never. Mixing demagoguery and science is irresponsible. It must never be tolerated.

OK, let's be more blunt.

The Federal Aviation Administration has long been criticised for its dual charter of both enforcing safety and encouraging the development of air commerce. The two roles are contradictory, representing an inherent conflict of interest. This does not reflect upon the character of the many skilled and motivated individuals that work there. But the agency's existence and function is based upon constraints that are often

defined by external parties, and the people that make up the FAA must work within those constraints. Just to make it clear, those constraints are "political," not "scientific."

In the specific case you find "deplorable," actions taken to challenge the operation of the ATR-72 in the US, the author makes credible points that external influences--namely, the ramifications of a bilateral accord, in which the US is obligated to accept the findings of the European airworthiness authorities; economic events which had nothing to do with the certification process; and French threats of reprisals against US aircraft--were factors in the FAA's action (or inaction).

Faced with such heavy-duty forces, the author exploited media interest in the October 1994 crash to point out what his concerns (as a pilot) were. He initially gave a public interview on a daytime talk show, and, eventually, churned out the book. He states he did so out of concern for the safety of the flying public. It is arguable that the media attention influenced the political climate. No bureaucracy wants to be seen as fallible, and it is equally arguable that ongoing pressure forced action on the issues.

I fail to see why this is unacceptable. Particularly given the criteria that you yourself have laid out, namely that it is an expert attempting to manipulate the system in his favor.

If we lived in a science-fiction world in which some mysterious quantity called Truth were feasible and easily obtained, then, yes, I

suppose we
could live in a quasi-fascist society in which the anointed
protect the
unwashed masses from the ambiguities of life.

However, we do not live in such a world. In our world, issues
often reflect
the vested interests of multiple parties, all of whom may be "in
the right,"
but who may nonetheless have conflicting agendas. There are
many checks and
balances in such circumstances. The government has competing
agencies
(e.g., NTSB vs. FAA) to ensure that institutional cultures do
not get out of
hand. The public can comment via its elected officials and the
free press.
The victims' families can react via their lawyers. If
information is
suppressed and kept in the province of "experts," the system
stops working.

Creating star chambers is not the answer, particularly when it
affects
operations in such a huge industry, in which MANY qualified
individuals are
in credible positions to comment, and, especially, in a
situation when SO
many peoples' lives can be put on the line.

I concede that investigation teams need room to work. The NTSB
freely
concedes that it must make periodic reports on the status of its
investigations. It does not issue a probable cause statement
until the
final report is issued. However, your model implies that no
discussion
whatsoever should take place until that final report is
released. That's
just unrealistic, in my opinion. It is contrary to safety and
even ignores
the interests of the affected parties--particularly the
traveling public.

Robert Dorsett <rdd@netcom.com> Moderator, sci.aeronautics.
simulation
aero-simulation@wilbur.pr.erau.edu [ftp://wilbur.pr.erau.edu/pub/
av](ftp://wilbur.pr.erau.edu/pub/av)

✈ AT&T -- Lessons forgotten

<Bob_Frankston@frankston.com>
Sat, 14 Sep 1996 12:38 -0400

Just got my brand new AT&T residential long-distance statement.
Of course, I
pay "electronically". The quotes mean that I do it through my
fancy computer
with Internet connectivity. And then the check gets printed out
on wood
pulp, physically hauled in a mail sack to AT&T's post office
box, removed
from the envelope, and then some clerk (automated?) keys it in
and credits
it to my account.

As error-prone as this process is, it sort of worked since the
account number
had a check digit which gave some hope of correctly crediting
the account. My
new account number no longer has the additional digits which,
I'd assumed,
were a combination of unique code and check digit. Now a single
slip of a
keystroke and my check gets credit to another's phone bill. But
at least, the
new bill is pretty with an Olympic logo and AT&T's corporate
logo. Who cares
about the data.

To be honest, it isn't clear that companies really used the check
information anyway. The attitude, as with credit card companies,

seems to be
deposit and, if someone complains, and verifies by showing the
back of a
physical check (which banks try to not provide any more), you
might convince
them that you really paid and they just miscredited it.

One day, in the far far future, there may be a course in "data
integrity" as
part of the accounting or MIS curriculum Until then, may your
checks find
the right home more often than not.

✶ Word for Windows risks, continued

JEREMY J EPSTEIN <JEPSTEIN@cordant.com>

Mon, 16 Sep 1996 11:22:57 -0500

In [RISKS-18.44](#), Edward Reid explains how Word saves files. But
it's worse
than what he describes. I'm working on a Word 6 document (under
Windows
3.1), trying to excise some references to obsolete terms. I
searched for
and deleted all of the references, and did a "Save As" to ensure
that I'm
creating a new file without any "leftovers" from earlier
versions. Doing a
search doesn't find any references to the deleted terms, but the
"Find File"
option (and utilities such as Norton Desktop's SuperFind) still
locate the
supposedly deleted text. So I presume they're somewhere in the
file, which
gives me very little confidence in the safety of handing someone
a Word
file.

The difference between this and previous discussions of the

topic (I believe) are that others have indicated that doing a "Save As" or disabling the "Fast Save" option would avoid this behavior. That's clearly not the case, for at least some versions of Word.

✶ Re: Microsoft VC++ property pages guaranteed to crash first time

John Vert <jvert@MICROSOFT.com>

Sun, 15 Sep 1996 17:01:54 -0700

Aside from the gratuitous insults, the below RISKS posting is also factually incorrect in a number of places.

The resource modification done below is **NOT** a modification to the file on the disk. It is done via a copy-on-write mechanism. The page containing the modified resource is written out to the paging file, not back to the original image. So there is no difference in the exe and whatever you ship to production IS THE SAME AS THE ONE THAT WAS TESTED.

Writing to a read-only resource does not cause a crash for the customer. The default unhandled exception filter for any Win32 application handles access violations caused by writing to a resource by changing the protection on the page from read-only (the default for resource sections) to copy-on-write and restarts the instruction. It will now succeed, but the modified page is written to the paging file instead of back to the original image. For more gory details, see KB article Q126630 "Resource

sections are
read-only" at <http://www.microsoft.com/kb/developr/win32dk/q126630.htm>

There are two reasons this behavior will cause you pain. You will see a first-chance exception if you are running under a debugger and have the debugger configured to handle first-chance exceptions for access violations.

If you don't understand the difference between first-chance exceptions (exception filter functions have not executed) and second-chance exceptions this can be confusing.

<http://www.microsoft.com/kb/developr/win32dk/q105675.htm> should help you out here.

Second, if your code has a filter function that handles this exception before the top-level exception filter sees it, the right thing is not going to happen. This is a RISK you always take when your exception filter handles exceptions it doesn't know how to handle.

-John

✶ Re: Microsoft VC++ property pages guaranteed to crash first time

Mark Mullin <mullin@taligent.com>

Fri, 06 Sep 1996 13:57:06 -0700

Microsquish Stealth Bug Insertion Technology

While I'm kind of dismayed by the "if you can't innovate, litigate" philosophy so often applied to Microsoft, this is a particularly

lethal
little gem from their MFC team. In many development environments, this problem will almost certainly guarantee that your app will crash the first time it is executed on customer machines, but the crash will only happen once, and will mystify tech support.

The problem arises in the use of property pages, otherwise known as tabbed notebook dialogs, as they are designed and implemented in the Visual C++/MFC environment. VC allows the developer to use interactive resource editors to design the property pages, but IT ONLY DOES THE FINAL STEP OF THE PROCESS IN EXECUTING THE APPLICATION, not in the development cycle. This step, where the style of the page is changed in the resource will cause most machines to abort the software as it is attempting to change a read only resource.

What really concerns me from a risks perspective is that the traditional development model is to release an exe to the test/qa group, and then to ship this exe to production when it receives a blessing from test/qa. This means that the exe shipped to production IS NOT THE SAME AS THE ONE THAT WAS TESTED, because the tested exe has been executed, and the one sent to production has not. Hence, every customer who launches the app for the first time will be rewarded with a crash, which can never be reproduced.

Yes, you can get around it with careful use of filtered exceptions. The problem is that this is rather insidious, and outside the realm of thinking

of most developers, who view an exe as the final product of the development

process. In this case, the final product is an executed exe.

Personally, I feel this is a lot like the Monty Python "Frog chocolates"

sketch. VC too should have a great big warning sticker on it saying "An EXE

from the linker is NOT A PRODUCT. YOU MUST EXECUTE IT TO MAKE A PRODUCT."

```
-- -- -- -- -- ORIGINAL MICROSOFT DOCUMENTATION -- -- --
-- -- --
```

Applies to class CPropertyPage, specifically the DoModal function that

causes the page to be presented on the screen.

```
virtual int DoModal( );
```

```
[... standard usage documentation deleted...]
```

```
[HERE IS THE INTERESTING BIT!!!]
```

Note. The first time a property page is created from its corresponding

dialog resource, it may cause a first-chance exception. This is a result of

the property page changing the style of the dialog resource to the required

style prior to creating the page. Because resources are generally read-only,

this causes an exception. The exception is handled by the system, and a copy

of the modified resource is made automatically by the system. The first-chance exception can thus be ignored. Since this

exception must be

handled by the operating system, do not wrap calls to

CPropertySheet::DoModal with a C++ try/catch block in which the catch

handles all exceptions, for example, catch (...). This will handle the

exception intended for the operating system, causing unpredictable behavior.

Using C++ exception handling with specific exception types or

using
structured exception handling where the Access Violation
exception is passed
through to the operating system is safe, however.

⚡ Re: Windows 95 passwords (Rochester, [RISKS-18.41](#))

Fieldhouse Dirk <Fieldhouse@logica.com>

Mon, 16 Sep 96 17:19:00 bst

> I clicked on "Cancel" in the dialog box and ... I was granted
access.

The system could have been configured so that it would have been
difficult
for you to do anything as a default user (in particular, it
could have
logged you off immediately).

Windows 95 security may not be its best aspect, but even a
certified secure
product is only secure with respect to its security claims and
only then
under certain conditions - eg, the procedures in the
accompanying Trusted
Facility Manual must be followed. You have just seen an insecure
default
configuration - basically what many Unix suppliers have provided
for years.

Dirk Fieldhouse, Logica UK Limited, 75 Hampstead Road, London
NW1 2PL UK
fieldhouse@logica.com +44 (171) 637 9111

⚡ Re: AOL curbs incoming spams (Clapper, [RISKS-18.42](#))

Bernard Peek <bap@intersec.demon.co.uk>

Fri, 13 Sep 96 20:58:25 GMT

> In the Supreme Court decision, the Court said that our right
to be
> bothered does not justify limiting First Amendment rights.

However there's an interesting interaction between US and UK
laws here. We
have a Computer Misuse Act which makes it an offence to alter
any data on
any computer without proper authorisation. If I declare that
unsolicited
e-mail advertising to this node is unauthorised (and this I
hereby do) then
anyone sending such mail to me is committing a criminal offence.

The US telephone service is required, under international
treaties, to
prevent this.

Bernard Peek bap@intersec.demon.co.uk

I.T and Management Development Trainer to the Cognoscenti

✶ More thoughts on junk mail

Mean Green Dancing Machine <aahz@netcom.com>

Fri, 13 Sep 1996 16:51:57 -0700 (PDT)

In all the discussions on junk snail mail I see, there are many
comments
about the time required to sort through it (which may or may not
be the
basis for a legal case), but I've seen few comments about the
direct cost of
throwing away the junk mail.

If we can enact a junk fax act on the basis of direct cost, we
can

probably do so for snail junk as well.

Aahz (@netcom.com)

✶ Re: Sometimes junk e-mail is already a fax (Franklin, [RISKS-18.45](#))

Mark Eckenwiler <eck@panix.com>

13 Sep 1996 21:47:59 -0400

Having tried to quash this theory repeatedly, I'm discouraged to see it re-emerge yet again in RISKS. The fact is that courts are not going to read TCPA as applying to junk e-mail. Most of the reasons are set out in the NetGuide article whose URL I gave in my previous message. I won't repeat those arguments here, but here are two I didn't have room for in print:

1) Section 227(d)(1)(B) of Title 47 makes it illegal

to use a computer or other electronic device to send any message via a

telephone facsimile machine unless such person clearly marks, in a

margin at the top or bottom of each transmitted page of the message or

on the first page of the transmission, the date and time it is sent

and an identification of the business, other entity, or individual

sending the message and the telephone number of the sending machine

or of such business, other entity, or individual.

Note this section applies to noncommercial messages as well as commercial ones.

If a computer equipped as described by Dan Franklin were really a TFM for purposes of the TCPA, then almost every Usenet post (and a vast amount of e-mail) would be illegal, since it is highly unusual for senders to put their telephone numbers in the headers. (I leave aside entirely the problem of what a "page" is in an e-mail message, other than to observe that this is further evidence that Congress had only conventional faxes in mind.)

BTW, it is not an adequate response to say "oh, but 'telephone number' here just means your correct e-mail address." If you're not willing to read "telephone number" literally, why on earth should anyone adopt a hyperliteral reading of the definition of a TFM in sec. 227(a)?

2) Suppose someone in your company sends e-mail to the two dozen people in his/her working group advertising a bake sale or yard sale. Assume further that a single recipient reads this e-mail on a networked PC equipped with a modem and printer. Under the proposed broad reading of the TCPA, this would be illegal. Is that what Congress intended? (The legislative history certainly doesn't offer any support for it.)

FWIW, there are no cases addressing this question of whether junk e-mail is covered by the TCPA. Frankly, I think the issue will be moot before very long; this is too hot (and vote-getting) an issue to be ignored by Congress, which has been more than willing to legislate rules for the Internet this year.

Mark Eckenwiler eck@panix.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 18: Issue 47

Thu 19 September 1996

Contents

- [Electromagnetic interference, medical-device risks, and airplanes](#)
[PGN](#)
- [Lexis' P-Trak vs ptrax](#)
[Emma Pease](#)
- [Re: Minnesota disconnected from the world](#)
[Theodore M.P. Lee](#)
[Jeremie Kass](#)
- [Re: Microsoft VC++ property pages guaranteed to crash](#)
[Boyd Roberts](#)
- [More ATM risks](#)
[Rory Chisholm](#)
- [411 needs 911](#)
[Kent Quirk](#)
- [Bringing Home the Anonymous Bacon](#)
[Peter Wayner](#)
- [Risks of not including appropriate manual overrides](#)
[William Hutchens](#)
- [Re: Failure-mode risks revealed by Hurricane Fran](#)
[Steve Holzworth](#)
- [Ariane 5 report, available on line](#)

[Richard J. Fateman](#)

● [ETHICOMP96 MADRID 6-8 November 1996](#)

[Centre for Computing and Social Responsibility](#)

● [Info on RISKS \(comp.risks\)](#)

✶ Electromagnetic interference, medical-device risks, and airplanes

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

Tue, 17 Sep 96 18:29:21 PDT

INTERFERENCE WITH MEDICAL DEVICES

There is an article on the effects of interference on medical devices, ``Electromagnetic interference and medical devices'', *Health Letter*, Public Citizen Health Research Group, 12, 6, June 1996, pp, 6-7. Apnea monitors have failed to sound the alarm when patients have stopped breathing. At least one implanted defibrillator has failed, responding to EMI and delivering a shock to a normally functioning heart. Power wheelchairs have also been affected. The greatest risk still appears to be implanted heart pacemakers, for which various problems are included in the RISKS archives. EMI is particularly problematic in hospitals, where sensitive monitors converge with radiating equipment (e.g., high-frequency generators and electrosurgical, diathermy, MRI, and x-ray machines). Cellular telephones are also a serious concern as emitters. Wireless technologies are likely to make things worse.

The July 1996 issue of *Health Letter* summarizes the reports of

two more recent studies on the effects of cellular phones on pacemakers. In the first study, tests of analog phones (90% of today's cellular phones) showed minimal interference (3% of the time), while *all* of the digital phones caused some level of interference. In the second study, 30 types of pacemakers were tested. Motorola's MIRS (used in foreign markets) caused EMI in 36% of those pacemakers within 3.5 inches or less. North American Digital Cellular phones interacted with 10% of the pacemakers within 1.5 inches.

MISCELLANEOUS MEDICAL DEVICE SOFTWARE PROBLEM

Incidentally, the September 1996 issue of *Health Letter* notes a Class II recall of 7200-series microprocessor ventilators (in particular, 7200ae, e, and sp with certain serial numbers, 8402 in all), which can stop operating when they are first turned on -- due to defective software. The manufacturer is Nellcor Puritan Bennett, Carlsbad CA, 1-800-255-6773. (2987 units of the model 7200 are also being recalled because of a defective transducer that causes it to stop ventilation for certain data-dependent settings.)

INTERFERENCE WITH AIRPLANES

There is an excellent article on the effects of electromagnetic inference on airplanes: Tekla S. Perry and Linda Geppert, ``Do portable electronics endanger flights? The evidence mounts'', *IEEE Spectrum*, September 1996, pp. 26-33. Check it out. I learned a lot.

[ham@cs.utexas.edu (Hamilton Richards Jr.) summarized the
Spectrum

article as follows:

The risk that RF emissions from carry-on electronic devices
will affect
avionics, although not high, is still high enough to warrant
tougher
government regulations.]

⚡ Lexis' P-Trak vs ptrax (Re: [RISKS-18.44,45](#))

Emma Pease <emma@Kanpai.Stanford.EDU>

Fri, 13 Sep 1996 18:34:50 -0700 (PDT)

A copy of the warning letter crossed my display on 11 Sep 1996,
and
immediately triggered the feeling of don't trust the information
without
checking (the multiple levels of quoting by the time it got to
my desk for
instance). So, I decided to do some checking using alta vista
and dejaneux.

One of the first things I discovered was that the product in
question is not
called ptrax (though Lotus produces something with that name)
but rather
P-Trak and that warnings first went out in early June about it.
[1] Before
that time Social Security Numbers were visible, afterwards they
weren't
though they were still in the database. I also found the
description of the
product (date unknown, but I think June of this year).

<http://www.lexis-nexis.com/lnc/Products/media/issue396.html>

Lexis-Nexis also seems to have put the following up within the

last day
or so:

<http://www.lexis-nexis.com/lbcc/about/ptrak.html>

I also noted that the database lists the person's maiden name (not the person's mother's maiden name, as stated in the warning message), though given a large enough database a searcher might be able to figure out your mother's maiden name. [It is also typically on your birth certificate, which is public-record stuff. PGN]

Risks: Most of us seem to have accepted the message without much checking as even the simplest check should have turned up the correct spelling of the product name (though admittedly by phone p-trak and ptrax could sound the same). In this case, most of the information was correct -- but will this always be true?

Emma Pease

[1] See http://www.epic.org/alert/EPIC_Alert_3.12.txt (The Electronic Privacy Information Center, June 25th newsletter). See also C-Net

<http://www.cnet.com/Content/News/Files/0,16,1527,00.html>

<http://www.cnet.com/Content/News/Files/0,16,1539,00.html>

for some articles on the matter in June.

[There are lots of items on this subject in today's media. Also,

sidney markowitz <sidney@research.apple.com> notes the web address of

<<http://www.lexis-nexis.com/lbcc/p-trak/p-trak.html>>

has a form to fill in and submit on-line, to remove

yourself. PGN]

⚡ Re: Minnesota disconnected from the world ([RISKS-18.46](#))

Theodore M.P. Lee <timplee@MR.Net>

Wed, 18 Sep 1996 22:02:39 -0500

Official statement form MR.Net, 16 Sep 1996, sent to a technical list:

> InternetMCI's network experienced periodic outages on national scale from
> approximately 3:30am til 10:00pm CDT yesterday. The effects of the outage
> were not uniform network wide. MRNet was one of the harder hit, CICNet and
> NorthWestNet were also badly hit. The Seattle area seems to be the hardest
> hit. Some InternetMCI customers are said to have seen nothing but slow
> downs. At one point the BGP routing to several of NAPs were affected.

> The outage was caused by a bug in Cisco routers that was triggered certain
> network events. The nature of these events and why they have not shown up
> until now has not been determined. InternetMCI is still investigating all
> the data gathered from the failure, until this is complete nothing is
> being suggested or ruled out."

[swb@mercury.campbell-mithun.com (Shawn Barnhart) updates Ted's R-18.46

message, noting that *not all* of Minnesota gets its connection through

MR.Net -- Minn-Net and at least one other use uu.net. PGN]

✂ Re: Minnesota disconnected from the world ([RISKS-18.46](#))

Jeremie Kass <jeremie@umich.edu>

Tue, 17 Sep 1996 23:30:06 -0400

We at U of M were disconnected from the world for more than 12 hours.

Starting at ~5am on Sunday the 15th, MCI was upgrading their routers. The engineer I talked to at the the MCI NOC said that something went wrong during the upgrade and all the software (I'm not sure if it was the actual software, or the routing information) was fried. Our connectivity to the Internet was pretty much gone at that point ... some of MCINet's peerings worked as we could get to msn.com, but not to microsoft.com. To compound problems, at about the same time, PSINet lost two of their BGP routers at MAE-East & MAE-West. This affected me since many of my customers & our corporate network are on PSINet, so I couldn't get to PSINet from MCINet (actually, mich.net, the academic ISP for Michigan) since their peering was at MAE-East.[*] By Monday morning all was resolved, including PSINet's problems.

Happy ending to a bad weekend for the 'net, but at least the engineer I talked to at MCINet was able to joke about it.

Jeremie Kass, Information Technology Consultant, Ciara Systems, Inc.

University of Michigan jeremie@umich.edu * jeremie@ciaraweb.com

[* I would have thought they were peering at MAE-West.

You know, "Come up and C(++) me some time." PGN]

✶ Re: Microsoft VC++ property pages guaranteed to crash ([RISKS-18.46](#))

Boyd Roberts <boyd@france3.fr>
Wed, 18 Sep 1996 12:06:14 +0200

Reading the article written by John Vert <jvert@MICROSOFT.com> and then the two cited KB [Knowledge Base] pages it strikes me that the real RISK is the complexity of the software offered by Microsoft.

It is difficult to use many of the Microsoft API's because the things they act on are inherently complex. Often, to do a 'simple' thing you have to call multiple APIs and many of these have a non-trivial number of arguments and/or must be passed complex data structures. In many cases these parameters set to 'defaults', so why have them in the first place? In any case, just how can all the combinations be tested?

This situation is made worse by the incomprehensible documentation. I find that his article and the KBs verge on the incomprehensible. This is rampant through Microsoft documentation. I'm a University educated, native English speaker with 12 years in computing and much of the Microsoft documentation contains semantic contradictions, before it even gets to the technical level.

At the technical level one wonders why anyone would design it

they way it was designed [writing on a read-only object being permitting based on some perverse set of rules]. Combined with the confusing nature of the documentation you are left wondering if how you thought it worked is actually how it does work.

Sometimes, as a last, turgid, resort you just have to try it out and see how it does work and hope that you are using it in the way it was intended and in the right context. This is no way to write software. I don't want to hope that it works. I want to know that it works.

Looking at Windows 95 I see something that is maybe an order of magnitude more complicated than Windows 3.1, still only solving the same problem. Doing the same with more is not progress. Exploiting Moore's Law may be possible, but it's not desirable.

⚡ More ATM risks

<rchishol@math.ethz.ch>

Wed, 18 Sep 1996 21:00:44 +0200

Late last Monday night an interesting sight met me when I went to get cash from an ATM.

These ATMs come with a small color screen a numeric keypad with a cancel and an ok key, and 8 keys next to the screen. Normally you are first prompted to insert your card and type in your key, after which you are presented with a

graphical menu allowing you to redraw money, check your account balance
change your PIN or retrieve your card.

This time things were different. First the person in front of me left the
ATM cursing loudly. When I got there, instead of the graphical menu the
screen was black with characters in white, several lines of "bad command or
filename" ending on a "C:\exe>" prompt.

After a little experimenting I found the keys 0-9 were mapped, as expected,
to 0-9, while the OK key was mapped to <ret> and the CORRECT key was mapped
to . The keys next to the screen (of which there were 8) turned out to
be mapped to A,B,C,D,..,<esc> respectively, with the 2 last keys apparently
doing nothing. Since I didn't have a full keyboard, and lacked an <alt> key
I couldn't enter anything useful, so after some brief experimenting I left
it alone. I then called the banks 24 hour hot-line and told them their ATM
needed rebooting. I got a rather vague response along the lines of "oh well
just wait a few minutes and see".

The risks ?

Well where should I start...

1) It should never be possible for the user of an ATM to access it's operating
system (if ms-dos + win 3.11 was the operating system, if not it shouldn't
be possible to access to front-end either).

2) More to the point it shouldn't be possible to use anything but the
authentication program prior to authentication. Note that

during my

experimenting with the ATM I hadn't put my card in.

3) I had always assumed that ATMs ran some kind of well designed embedded

system. "Well designed" doesn't come to mind when talking about ms-dos.

I am on the other hand certain that a pc with dos/windows is the cheapest

way of building an ATM (cheap standard components, lots of programmers

available for the platform, cheap standard tools available for development).

What does this say about the general quality of the information resources

used by this bank ?

4) Does the bank ever run virus-scanners on the pc in the ATM ?
Having

one of these things infected could lead to all kinds of problems. Of

course virus-scanners are never 100% reliable.

Seeing the problems these machines seem to have, it is only fair for me to

report one occasion recently when my local ATM got something right: On

requesting a certain amount of money, the ATM always hands your card back

first, and then hands you the money. Last week my card jammed in the ATM and

I got neither card nor money. I went to the local branch of my bank

immediately, expecting to find the money I hadn't received deducted from my

account, but apparently it hadn't been, indicating that at least this time

the designers of said ATM got things right.

Rory Chisholm rchishol@math.ethz.ch

411 needs 911

Kent Quirk <kentq@world.std.com>

Wed, 18 Sep 96 14:13:51 -0500

My family and I have just recently returned from a year's assignment overseas and have moved back into our old house, which we rented out for the year. Of course, we gave up our old telephone number (though I kept my e-mail address -- first things first!). When we returned this year, it was easy to get a new phone number; they still had my old account information handy.

We've been gradually re-establishing contact with our friends. This week, two old friends told me that they'd been trying to call me, but that the number information gave them was "not taking calls at this time". I asked what number it was, and they told me our *old* number from last year! I called information (411 for local information) myself, and was given the correct number. I asked one of them to check again; again she was given our old number. She tried to explain that she KNEW it was the wrong number, and was told the equivalent of "Sorry, lady, that's what the computer says." She had dialed 555-1212 (the standard for non-local information questions)

I called NYNEX service to ask what was going on. She checked the records -- they were correct. With me on the line, she called 555-1212 and was given the right number. She explained -- reasonably -- that she couldn't fix a

problem that didn't seem to exist.

My friend tried again. Was again given the wrong number. She then explained, again, that the records were wrong. At my request, she asked for the information on exactly which company she was talking to and where they got their data. She explained that they were contractors for NYNEX, Then she asked my friend for the correct information so she could change it!

The RISKS? The usuals:

a) Assuming that old data is good data; somebody somewhere seems to have decided that the same name at the same address must have the same number.

b) Changing the data without having any proof at all that the new data is valid or that the change is authorized. Can you imagine someone doing this to a competitor? It was awfully easy.

c) Our assumptions that there is somehow, somewhere, God's database of telephone numbers managed and maintained by The Almighty Telephone Company, and that changes propagate intelligently. 'Taint so, folks.

So, I THINK that my phone number is now correctly stored in the information systems --- unless it gets overwritten by some other glitch somewhere else.

I guess I have to keep testing it for a while.

Kent Quirk, Acton, MA, USA kentq@world.std.com
Phone: Call information ... if you dare.

✶ Bringing Home the Anonymous Bacon

Peter Wayner <pcw@access.digex.net>

Tue, 17 Sep 1996 13:04:47 -0400

The *Baltimore Sun* reports in its 17 Sep 1996 issue that people in Baltimore are paying for drugs with meat (page A1! [pretty saucy!]). Perhaps this is not yet anonymous digital cash, but certainly anonymous.

[Now someone is going to propose keeping a database of all sides of beef, and steganographically watermarking the meat in the context of digitally signed scannable grade-stamps. Perhaps the next step in monitoring the private drug-meat trade would be to escrow the inspectors' private keys, derived from the product of two U.S. Primes, and put the database up on the net: the T-bone connected to the M-bone, etc.? PGN]

✶ Risks of not including appropriate manual overrides

William Hutchens <wthutchens@usa.pipeline.com>

Sun, 15 Sep 1996 05:44:01 GMT

Dave Schulman's recent contribution ("Failure-mode risks revealed by Hurricane Fran" [RISKS-18.42](#)) reminded me of an incident that happened to me a little while ago. Back in December 1995, I was interviewing for a residency position at a hospital in Toledo, and the hospital was being generous enough to put its applicants up in one of the better

hotels in the
city (which shall remain nameless).

The hotel had recently changed over to an electronic card system on their doors rather than the traditional lock and key system. The morning of my interview, I was coming back from breakfast, and was planning to get my suit jacket from my room and check out. When I got to my room, I inserted the keycard into the lock and, instead of getting the green LED and hearing the mechanism unlocking, I was greeted with a series of all three LED's blinking, in what I assume was an error code.

I went to the front desk and explained my situation to the manager who got the 'master key' card and tried it in my lock, and got the same response as my key. She went back to the front desk and put in a call to maintenance. A few minutes later, the maintenance man showed up with what was supposed to be a supermaster card. No dice, same result.

He went away and returned after a long wait with two other keycards. (He said that it took a while for him to get in touch with his supervisor who gave him some 'special codes'). He tried the two cards in the lock; they obviously did something since the LED's blinking pattern changed, but the lock still wouldn't open.

He went away again, and he then returned along with the manager and two other people. The manager pulled out a laptop computer connected to a probe which fit into the keycard slot. While she was working, one of the

two other people identified herself as the 'head concierge' and began furiously apologizing to me. The manager did succeed in opening the lock this time.

This anecdote illustrates a risk touched upon by Mr. Schulman -- the problems with not including a manual override in a computer controlled system. Had the laptop computer not been able to convince the lock to open, I don't know of any way short of brute force of getting the door open as there were no openings in the lock other than the keycard slot. (During the times I was left waiting in the hallway, I was half expecting the maintenance man to return with a sledgehammer).

Although I'm not intimately familiar with the internal workings of electronic locks, I don't believe that it would be a problem to include a conventional mechanical keyway in the lock. In the ideal system, the mechanical keys would be kept secure (say, in a safe in the office) and only the electronic cards would be given to guests. This would keep the advantages of the electronic locks (convenience, the ability to change locks easily whenever a guest leaves) without having to keep track of mechanical keys.

Bill Hutchens wthutchens@usa.pipeline.com

✉ Re: Failure-mode risks revealed by Hurricane Fran (Schulman, R-18.44)

Steve Holzworth <sch@unx.sas.com>

Fri, 13 Sep 1996 13:52:51 -0400 (EDT)

I must take exception to most of what Dave states here. I'm a life-time resident of North Carolina, and have lived in the described area (Research Triangle Park) in central NC for twenty years.

>The area was clearly unprepared for a disaster of this magnitude, ...

Was Florida prepared for Homestead? [>...]

1) Raleigh-Durham is over 100 miles inland from the coast. Hurricanes rarely effect the area with more than peripheral tropical-storm-type weather. Fran was a major exception to the rule. Flooding along the rivers and lakes here qualified as "200-year flood" waters, meaning that you should expect floods of this type only once every 200 years. Normal civil engineering for building sites relies on meeting the "100 year flood" limit in most cases.

2) Power lines are aerial still throughout much of Raleigh because Raleigh has been here a long time. It is impractical to bury all of the power lines due to the sheer number of miles of cable involved. Most subdivisions and other developments built in the last 15 years do have underground utilities. In Cary nearby, building codes require it.

3) The central NC area is covered in trees. Many of the streets in the area, particularly older parts of town, have large oaks with canopies extending over the streets. The trees are one of the things that gives the area its

charm.

Most widespread power outages were caused by the downing of high-tension distribution lines. More importantly, several gas leaks resulted from uprooted trees pulling lines UP out of the ground, so burial is far from a cure-all. Major trees are down throughout the central NC area. The storm had sustained winds of 67 mph in Raleigh, with gusts of up to 117mph. Remember, this is over 100 miles inland... [>...]

The telling point: "where hurricanes are an established fact of life." Much of Florida's vegetation is tropical, which is suited to severe winds and storms. In contrast, Raleigh is known as the City of Oaks. Many of those trees are over 300 years old. Many are uprooted or broken apart now.

Many power lines did come down. A week later, most people living in municipalities have power restored. While inconvenient, I can deal with a week of no power if the alternative is to cut down all of the trees anywhere near a power line. In the hurricane aftermath at Homestead, FL, some people didn't have power for months. [>...]

Having a sole entrance gate that fails closed is stupid, but not particularly unsafe. Virtually all mechanical entrance gates are designed with shear pins in the mechanism. In the event of fire, the fire department simply drives through the closed gates, that's what those big bumpers are for. Most municipalities here will not allow you to build a subdivision or apartment complex with only one entrance. A tree could have

blocked said
entrance just as easily as the closed gate.

Now compare this with the alarm system my neighbor's place of work has. He went to work to check on things in the aftermath of the storm. It turns out that after the backup battery on their system wears out (approx. 3 hours), the system OPENS all of the locks on the doors. Note that typical card-key-locked doors have a manual handle on the inside to open the door anyway if power is off, in addition to a mechanical key for entrance, so the risks of being locked in or out are minimal. In his case, NOBODY was locked out. Just what you need in the aftermath of a storm, when the opportunists are about. [>...]

It's a near miracle that more people didn't die, but it has nothing to do with the utilities. The height of the storm was at approx. 3:00 AM, so most people were at home. The eye of the hurricane went directly over Cary, approximately 7 miles west of Raleigh. Carolina Power & Light and Duke Power both scrambled to obtain line crews from other regional utilities even before the storm had gone through the area. They have reciprocal agreements with other utilities to supply crews in the event of an emergency of this nature. Everyone actually expected the problems to occur along the coast. BellSouth sent their generating units there to maintain power on their cellular towers. They were dismayed to find that the problems occurred exactly where they had just dispatched their crews from... While there was extensive damage at the coast, the major damage was actually

inland. Wake

County alone has estimated damage in excess of 900 million dollars.

Steve Holzworth SAS Institute Open Systems Cary, N.C.
R&D VMS/MAC/UNIX sch@unx.sas.com

✈ Ariane 5 report, available on line (Re: Frisbie, [RISKS-18.45](#))

"Richard J. Fateman" <fateman@peoplesparc.CS.Berkeley.EDU>

Fri, 13 Sep 1996 11:03:36 -0700

ARIANE 5 Flight 501 Failure, Report by the Inquiry Board,
The Chairman of the Board : Prof. J. L. Lions
is in fact available (in English) as
<http://www.esrin.esa.it/htdocs/tidc/Press/Press96/ariane5rep.html>

It is not that long, and explains that the proximate fault was a conversion of a 64-bit float to a 16-bit integer. [See [RISKS-18.27, 28, 29, 45](#). PGN]

"The internal SRI [inertial reference system, en francais] software exception was caused during execution of a data conversion from 64-bit floating point to 16-bit signed integer value. The floating point number which was converted had a value greater than what could be represented by a 16-bit signed integer. This resulted in an Operand Error. The data conversion instructions (in Ada code) were not protected from causing an Operand Error, although other conversions of comparable variables in the same place in the code were protected. "

The circumstances surrounding the code, testing, simulation,

etc., are probably worth reading, though the suggestions as to how to prevent such problems in the future are mostly nontechnical, and where they are technical, do not provide any great insight, unfortunately.

Richard Fateman, UC Berkeley

✶ ETHICOMP96 MADRID 6-8 November 1996

Centre for Computing and Social Responsibility <ccsr@dmu.ac.uk>

Mon, 16 Sep 1996 20:39:07 +0100 (BST)

The third International Conference on Ethical Issues of Information Technology, University of Salamanca in Madrid, Spain

Two international conferences have been held which address these issues. The first was in the USA at Southern Connecticut State University and the second, ETHICOMP95 was at De Montfort University in the UK. Both conferences have been recognised as milestones in furthering the study and understanding of the societal and ethical issues of IT. ETHICOMP96 brings together leading international speakers to debate the current and future impact of IT and the societal and ethical issues consequently raised. Madrid is an ideal location for this conference as it is a major European capital with a high cultural, academic and commercial reputation.

* Keynote Speakers

Professor James Moor, Dartmouth College, USA

Reason, Relativity and Responsibility in Computer Ethics

Professor Porfirio Barroso, University of Salamanca in Madrid,
A European dimension to codes of ethics for the computer
profession

- * A. Organisation and society structure and the location of work
- * B. Privacy, property and computer misuse
- * C. Value and accuracy of data and information
- * D. Developing information systems now and in the future
- * E. The IT Profession
- * F. Education
- * G. Frameworks

Conference Administrator, Maria Angeles Nevado
Conference Chairman, Porfirio Barroso

Contact address: Porfirio Barroso (ETHICOMP96), Clinica Puerta
de Hierro,

San Martin de Porres 4, 28035 Madrid, Spain

Telephone and Fax: +34 1 3866775

(To send a fax when you hear the answer machine press START)

E-mail pbarroso@capilla.cph.es

To directly reach the ETHICOMP96 Homepage:

[http://www.cms.dmu.ac.uk/CCSR/ccsr/conf/ethicomp/
ethicomp96.html](http://www.cms.dmu.ac.uk/CCSR/ccsr/conf/ethicomp/ethicomp96.html)

[Centre for Computing and Social Responsibility, Dept of
Computer Science,
De Montfort University, The Gateway, LEICESTER, UK LE1 9BH
ccsr@dmu.ac.uk

<http://www.cms.dmu.ac.uk/CCSR/>] [This item excerpted 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 18: Issue 48

Monday 23 September 1996

Contents

- [An unlosable casino game](#)
[Kristiansen](#)
 - [When is \$-32768 \neq -32767-1\$?](#)
[Bear R Giles](#)
 - [RISKS of temporary change-of-addresses](#)
[Simson L. Garfinkel](#)
 - [AIDS list compromised](#)
[Winn Schwartau](#)
 - ["PRIVACY Forum Radio", Lexis-Nexis "P-TRAK" Interview/Update](#)
[Lauren Weinstein](#)
 - [Detailed Update Regarding Lexis-Nexis "P-TRAK" Database](#)
[Lauren Weinstein](#)
 - [Even more ATM Risks](#)
[James Robertson](#)
 - [SYN Floods, IP Spoofing, and what to do about it](#)
[Fred Cohen](#)
 - [More on portable electronics/airplanes](#)
[Peter Ladkin](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✶ An unlosable casino game

Kristiansen <ekristia@xs4all.nl>

Sun, 22 Sep 1996 14:37:03 +0200 (MET DST)

The Dutch radio station Radio 538 (<http://www.radio538.nl> [in Dutch] has set up a "Virtual Casino" on their web server, as a protest against legislation-in-the-making against Internet gambling.

The "casino" consists of a virtual slot machine. Playing is free of charge, and you can win real prizes, presumably paid by the sponsors whose company logos appear prominently.

So far so good.

The amusing part is that the constructor of the Web site missed one little detail: If you lose in a turn of the game, you just click on "BACK" on your Web browser, and you undo your loss!

Erling Kristiansen

[The object is probably to let you win, gaining free publicity. It would be a risk if there is no limit on individual winnings. But this should certainly be a reminder to future webgame developers. PGN]

✶ When is -32768 != -32767-1 ?

Bear R Giles <bear@indra.com>

Fri, 20 Sep 1996 15:07:31 -0600 (MDT)

We have recently started using the Borland 5.01 C/C++ compiler

[*], and came across an interesting anomaly. The minimal "short" integer, as defined in the ANSI-standard file <limits.h>, is -32768. Curiously it is defined as "(-32767-1)".

At first I attributed this format to symmetry; the maximum "short" small integer was defined as 32767. However I soon noticed "long constants" and "possible loss of precision" error messages with any code which initialized a "short" integer to -32768. If this were human generated code, these values could be easily changed to "SHRT_MIN", but this code was state tables output by Gnu Flex.

Turning off these error messages is risky since a fair number of bugs (in my experience) are related to precisely this type of logic flaw, especially when the software needs to run on multiple platforms. On the other hand, leaving the error messages enabled prevented me from compiling this program, due to "excessive errors or warnings."

Still, this situation is better than I would face when using a personal copy of Microsoft Visual C++ 1.5. It limits SHRT_MIN to -32767.

[*] A bit of research shows that the problem goes back to a least Borland 4.0.

Bear Giles bear@indra.com

RISKS of temporary change-of-addresses

"Simson L. Garfinkel" <simsong@vineyard.net>

Fri, 20 Sep 1996 12:30:28 -0600

For the past year I've lived on Martha's Vineyard, but I spent the summer in Boston. Eager to have my mail forwarded the 80-mile jump, I filed a temporary change-of-address with the US Post Office. The forwarding order expired on September 4th.

Now, it has been widely reported here and elsewhere that the US Post Office sells its national change of address register to the nation's top bulk-mailers so that they can automatically update their addresses. I've also documented how this information is used for target-marketing purposes, even though such uses are strictly forbidden by the Post Office.

What I discovered this summer, though, was that either the Post Office or the users of the databank do not distinguish between temporary change of addresses and permanent change of addresses.

During the summer, I had many magazines and financial statements delivered with the "corrected" address, which was a rented post office box in Boston. I had my insurance company call me up and ask me why I had moved without telling them. I had a lot of confusion.

What makes the confusion all the worse is that my rented mail box was canceled a week after the mail forwarding order was canceled. All mail sent there will be returned-to-sender. And, no, the post office will not forward paper mail that is destined for a rented post office.

Now I'm trying to find every company that I do business with that updated its copy of my address, and tell them that they shouldn't have updated the address, even though they thought they were doing the right think. All of this has been a huge waste of time --- not just mine, but the roughly three dozen companies that I've had to deal with.

What is the most frustrating, though, is that I did everything exactly the way I was supposed to, and still I got screwed by the system. On the other hand, I don't see any way that I could have gotten my mail forwarded and not had to suffer with these problems.

Simson Garfinkel PO Box 4188, Vineyard Haven, MA 02568. 508-696-7222

<http://www.packet.com/garfinkel>

⚡ AIDS list compromised

<winn@Infowar.Com>

Fri, 20 Sep 1996 16:10:59 +0100

The names of over 4,000 AIDS patients were secreted out of a Pinellas County, Florida, computer and sent to the *St. Petersburg Times* on 18 Sep 1996. William B. Calvert III, 35, one of only three people allegedly with access to the computer containing the files has been placed on administrative leave (with pay!) while investigations continue.

The computer disc was accompanied by an anonymous letter claiming that Calvert had been showing and bragging about the disc and its

contents at a
Treasure Island gay bar, Bedrox. The *St. Pete Times*^a said they
did not look
at the names on the list.

Preliminarily, the security controls over the list are said to
have included:

- A double-locked room
- A computer (no type specified) with a lock (unspecific)
- A single-attempt password system. (no specifics.)

I have been talking to the local reporters to see if we can
determine any
additional details like:

- Is there any other connectivity to the machine, despite the
locked room?
- Are there audit records?
- What were the real security controls
- Why there was no encryption
- Why officials do not consider such data bases confidential.

This story is making major headlines here in the St. Pete area
where I live,
especially since no one knows how many other disks have been
circulated and
where they might be sent, or worse posted. According to some
reports,
Calvert was a disgruntled employee, with a history of
allegations.

This one incident may be the largest single case of AIDS related
disclosures
ever. In 1993 a Miami data base of 6,000 HIV positive people was
stolen, but
investigators said the list was a corollary part of a hardware
theft.

The RISK we face, beyond the obvious leakage of the names and
the possible
disruptions of people's lives already disrupted by this terrible
disease, is
that others may not come forward for testing and treatment for

fear that their
names, too, will be publicized.

Winn Schwartau - Interpact, Inc. Information Warfare and InfoSec
V: 813.393.6600 / F: 813.393.6361 [Http://www.infowar.com](http://www.infowar.com)
Winn@infowar.com

✶ "PRIVACY Forum Radio", Lexis-Nexis "P-TRAK" Interview/ Update

Lauren Weinstein <lauren@vortex.com>
Sun, 22 Sep 96 23:22:10 PDT

In the message following this one, I've provided a detailed update on the current Lexis-Nexis "P-TRAK" personal information database furor, based on my own research. Since the situation has been changing very rapidly, this represents the most up-to-date information I'm aware of regarding both the service and your options for dealing with it if you so choose.

With concerns over databases and personal information running at such a high level, this seems like the appropriate time to announce the first program from the PRIVACY Forum's new effort: "PRIVACY Forum Radio". As longtime readers of the forum know, one of my major concerns is getting the word out to people that privacy really matters, and that there are actions they can take to help protect themselves, **before** troubles arise. Whether related to computer, telecommunications, or database privacy issues, or the less esoteric aspects of privacy in our personal lives, to be forewarned is

critical.

PRIVACY Forum Radio will be an ongoing production of the PRIVACY Forum. It initially will include audio interviews, discussions, and other programs conducted with all manner of persons involved in the privacy, security, and related areas. Participants will include persons from business, industry, government, concerned organizations, and other individuals. Both the well-known "movers and shakers" and the unknown folks affected by privacy problems will be featured. All aspects of privacy in our personal, commercial, and public lives will be topics for various guests. Initial programs will be prerecorded, but shortly we'll begin live broadcasts offering listeners the ability to call in by phone, or send in e-mail queries, to directly participate in the discussions.

The primary distribution medium for these PRIVACY Forum Radio materials is the Internet, via the Xing "Streamworks" system. Versions of the shows, including live programs, will be available for access by listeners at network connection rates as low as 14.4 Kbps per second. Some materials will also be made available at higher rates for those with the appropriate capabilities. In the very near future, we also plan to make some items available with accompanying video ("PRIVACY Forum TV"), using the same system.

These shows are also available, by arrangement, for conventional radio syndication. Since my primary goal is to try get the word out

about these issues as widely as possible, PRIVACY Forum Radio is also making available a short (e.g. 60-second) "Privacy Bites", suitable for use by regular broadcast radio stations who want to help their listeners not only become aware of privacy risks, but to learn what they can do about them. Inquiries regarding any of these materials should be directed by e-mail to privacy-radio@vortex.com, or by voice to (818) 225-2800.

The first special program from PRIVACY Forum Radio is an interview I conducted a few days ago with Lexis-Nexis Corporate Counsel Steven Emmert, on the subject of concerns over the "P-TRAK" database, and on the topics of personal information and databases in general. It provides fascinating insight into views of privacy from the "database industry" side of the fence. To hear this program, follow the PRIVACY Forum (and PRIVACY Forum Radio) links from

<http://www.vortex.com>

Links are present within the PRIVACY Forum Radio area explaining the technical details of hearing the interview and other materials, and for downloading the (free) Streamworks software for your system that you'll need if you don't have it already.

This is an exciting step in the evolution of the PRIVACY Forum, one that I'm hoping will be a major stride towards helping people worldwide deal with the ever-encroaching loss of privacy that has become part and parcel of our modern societies. Please direct any questions about accessing

or obtaining
PRIVACY Forum Radio materials to the e-mail address or phone
number
mentioned above. Thanks much!

--Lauren--

✦ Detailed Update Regarding Lexis-Nexis "P-TRAK" Database

Lauren Weinstein <lauren@vortex.com>

Sun, 22 Sep 96 23:22:58 PDT

This is going to be a longish message, but I urge you to read it in its entirety. As many of you are no doubt aware, considerable controversy has been raging around the Internet, and now in the mainstream press, concerning the Lexis-Nexis "P-TRAK" personal information database. Since the transmission of P-TRAK related messages here in the PRIVACY Forum early this month, various information, some accurate, some inaccurate, has been widely disseminated. In some cases, I've seen versions of the original PRIVACY Forum items in excerpted and usually unattributed form, sometimes having been modified or addended in manners that significantly alter the original content.

Concern over P-TRAK has mushroomed around the country, perhaps especially due to Lexis-Nexis' high visibility. Many people are concerned about their personal information, however innocuous some might consider it to be, residing in publicly accessible databases. They want some measure of

control over their personal data. It is this concern that has brought this story to national prominence.

Lexis-Nexis has put forth an official statement concerning P-TRAK (accessible via <http://www.lexis-nexis.com>) which is accurate as far as it goes--but in my opinion leaves out some *very* important points which people should be aware of and that I'll describe in detail below.

Adding to the confusion is the fact that over the last couple of weeks the mechanisms available for people to request removal from the P-TRAK database have been changing, largely due to the high volume of requests that Lexis-Nexis has been receiving. Callers to various Lexis-Nexis numbers were at times told conflicting or apparently inaccurate information, and the exact mechanisms for requesting removal, and what such a request really meant in practice, has been in a state of flux.

Early deletion requests were taken by operators, then by voicemail systems, and then later callers were told all requests had to be by mail or fax. Most callers were asked for their Social Security numbers. Some were told that it was essentially useless to request removal, since they could easily pop right back on the database again later. Questions about how to verify removal persisted.

Given all this, I decided to take it upon myself to go directly to the source, and had a number of detailed conversations with the Lexis-Nexis Corporate Counsel, Steven Emmert. Since Lexis-Nexis was in the process of

making decisions on some of these issues, I held off this update until now to give Mr. Emmert time to get me the latest information, which he has done.

As described in the previous message, I'm also pleased to announce that PRIVACY Forum Radio is presenting a detailed audio interview with Mr. Emmert, via the PRIVACY Forum web page (access via <http://www.vortex.com>).

Mr. Emmert and yours truly discuss both the details of the P-TRAK controversy and some of the more philosophical aspects of personal information databases. If you're at all concerned about these topics, you will probably find the interview quite interesting.

Where do the P-TRAK issues stand right now? First off, it should be noted that Lexis-Nexis is a reseller of the data in P-TRAK, not the collector. They don't verify or otherwise amend the original information. The information itself is the so-called "credit header" data which FTC and other decisions ruled were not covered under the FCRA (Fair Credit Reporting Act) and could be openly disseminated. This includes name, address, phone number, Social Security number, and other related data. Lexis-Nexis obtains this info from one of the big credit data agencies (published reports have suggested that this is Transunion). Lexis-Nexis receives this data, which includes more than 300 million records, on a monthly basis.

While Lexis-Nexis notes that their marketing focus is to government, law enforcement, and the legal profession, it's important to realize that the P-TRAK database is not *restricted* in any way to ensure that

only persons in those categories are using the data. Anyone who wants to pay the appropriate fee can obtain search data. This is a crucial problem in the database industry--the almost total lack of even rudimentary "need to know" requirements before gaining access to information that many persons consider (obviously erroneously in many cases!) to be private.

Lexis-Nexis points out that you cannot view Social Security numbers through P-TRAK. This is true. When the database was originally established in June of this year, SS#'s were available for viewing, but in short order concerns led to their display being terminated. So, you can't derive a SS# from someone's name via P-TRAK.

HOWEVER--this does not mean that SS#'s are not in the P-TRAK database. In fact, they are there, and if you already have an SS# you can use it to search in P-TRAK for all of the other data associated with that number (e.g., name, address, phone number, and so forth). Lexis-Nexis considers the SS# to be the only reliable personal identifier, and in fact has told me that when a person requests removal from the P-TRAK database (more on this below) the best chance of actually getting removed exists when that person provides their SS#. Name and address are considered less desirable for this purpose, due to name duplications, name or address changes, etc. This is the reason that callers asking to be removed have typically been asked for their SS#'s.

To Lexis-Nexis' credit, it should be noted that they have

competitors (some on the Internet) who don't restrict SS# information at all, and don't offer any opportunity to be removed from their databases either. Still, it's important to understand that SS#s *are* in the P-TRAK database, and that you still can search *by* SS# in that database.

Information available for direct view in P-TRAK includes name, maiden name (if any), current address, up to two previous addresses, phone number, and year/month of birth. Mother's maiden name is not included. The source of phone numbers is of particular interest. Lexis-Nexis in their statements has likened all this data to the telephone company "white pages", pointing out that it is all based on publicly available information. But the definition of "publicly available" is very broad--much broader than most people realize.

Phone numbers in P-TRAK are *not* derived from telephone company (e.g., white pages) information. They are obtained from a variety of other sources, notably data provided by businesses that have conducted transactions or other business with a person, to whom that person may have provided their phone number. As such, unlisted (non-published) phone numbers *can* appear in P-TRAK, since an unlisted designation only affects phone company records, not all the other places where you have provided a number, probably with the expectation that the number would not be provided to commercial databases! There are no legal restrictions on the dissemination of such phone numbers, even though many persons keep their

phone numbers unlisted for quite valid and serious reasons.

OK, let's say you've decided that you consider the information in P-TRAK to be significant to you, and you want your record deleted. First off, be aware that it could take up to 60 days for a deletion to occur. This is due to the 30 day cycle on the database source; the deletion request needs to be present long enough for a complete cycle to process.

Can you verify (for free) that a deletion has taken place? No, not easily; you need to pay for a regular P-TRAK search. Previously there was a contact person for verification of deletions, but due to the high volume of requests that option is apparently no longer being offered.

Will you stay off the list once a deletion request has been processed? Maybe. It would seem to depend strongly on how much information you provided with your original request. If you provided a SS#, you probably have a better chance of not finding yourself with a new record in a future cycle due to non-identical name or address information appearing for you in a future load of incoming data. Do you want to provide your SS# with your request for deletion? That's a personal decision of course.

What if perchance you don't currently have a record in P-TRAK? Will your deletion request be held until a record does come in? No, it will not. If you don't have a matching record at the time your deletion request is processed, that request will be flushed, and if a record for you appears in future data that record will enter the P-TRAK database. There

is no mechanism present for a "permanent" deletion request that would deal with such situations.

As noted above, the methods for requesting deletion have changed over the last two weeks. In fact, they've even changed in the few days since the recording of the interview with Steven Emmert (a different fax number and the re-establishment of voice requests on a new number). So be sure to use the information specified below, not the number that Mr. Emmert provided during the interview.

The following is the most up-to-date information as of this writing, and comes directly from my communications with Lexis-Nexis. Here are your options:

Telephone (toll free): 1-888-965-3947

Please note that this is a new number at Lexis-Nexis and is not scheduled to be working until this Monday morning (9/23)

Eastern Time. It is currently scheduled to go to live operators, but if volume is very high it might be switched to voicemail.

FAX (toll free): 1-800-470-4365

Again, this number is scheduled to become functional on the morning of 9/23, Eastern Time.

Mail: P-TRAK, P.O. Box 933, Dayton, OH 45401

E-mail: p-trak@prod.lexis-nexis.com

A web form for removal requests is also available at Lexis-Nexis via <http://www.lexis-nexis.com>.

The minimum information required to request removal is full name

and mailing
address. As noted above, Lexis-Nexis feels that the strongest
likelihood of
a successful removal will occur when Social Security number is
also provided.
The web form (as of this writing) doesn't request SS#, and you
of course
should use your judgment about choosing to send your SS# in e-
mail. My own
recommendation would be to use the telephone or fax options.

By no means is P-TRAK the most onerous database of personal
information
now available. But I believe the furor that has erupted
demonstrates
the deep-seated concerns that many people have with details of
their
personal lives being collected and sold merely as "information
commodities", with the subject of that data having virtually no
input
on how it will be used, or abused.

It's time for a detailed examination of what information should
and should
not be considered to be "public", who should have access to that
data, and
under what circumstances. Some database companies themselves
admit that this
is not an area that they can unilaterally address in any general
way--they
have competitive concerns. Only through serious legislative
efforts can we
really begin working toward reasonable changes in the commercial
database
field. And we'd better get started now, unless we want the 21st
century to
be a time when the word "privacy" becomes nothing more than an
amusing
anachronism in the history books.

--Lauren--

P.S. Be sure to check out my audio interview with Steven Emmert

of

Lexis-Nexis on PRIVACY Forum Radio if you can. Just follow the PRIVACY Forum links from <http://www.vortex.com> to PRIVACY Forum Radio.

["Michael J. Chinni" <mchinni@PICA.ARMY.MIL> noted a change in the web address reported by Pease in [RISKS-18.47](#). He suggests searching down from main address, noted above. PGN]

✦ Even more ATM Risks (Chisholm, [RISKS-18.47](#))

James Robertson <jamesr@desklaw.com.au>

Mon, 23 Sep 1996 22:15:24 +1000

Rory's description of his close encounter with a dodgy ATM machine reminded me of a more than annoying incident I suffered recently.

Needing to withdraw a large amount of cash in a hurry, I went to my local ATM machine, and requested \$700.00 in cash. The machine normally gives out \$20.00 or \$50.00 notes, and obviously I was expecting the latter.

Unfortunately, it gave me the former. Of course, this consists of 35 bills.

It spent some time shuffling bills behind the scenes (which was where I started to get the idea that something was not well). Some clunking noises later, and it gave me some bills. Eleven of them to be exact. It then gave me a receipt.

Needless to say, it deducted the full \$700.00, even as I could hear it withdrawing the bills back into the bowels of the machine.

The cause: it simply couldn't fit that many bills through the slot. So it sent through what it could, and took back the rest.

The RISK: Somewhere in the bank there are teams of programmers, writing and maintaining the software for the ATMs. They handle many types of exceptions, and error conditions.

Elsewhere, there are many engineers, carefully poring over the design of the ATM, its cash dispenser, checking that there are no foulups, or possible causes of mechanical failure.

Then there is the person who takes the hardware, loads the software, and sends the ATM out. The programmers never see an ATM (except when they are withdrawing their money), and are likely never told its physical characteristics.

Similarly, the engineer is simply told that some software is loaded on the computer that he (or she) has bolted into the case.

I'm sure it has just not occurred to the managers that mere physical constraints can affect the operation of ATM software ...

The even greater RISK? How do I get a message to the programmers responsible for the problem? There is no mechanism in the bank for you to write a complaint to the support staff. And what do you think are the chances of them having the time to think about the problem and discover the cause for themselves?

James

PS. It took over a week for them to finally get my money back into the account. Several checks almost bounced as a result.

James Robertson * jamesr@desklaw.com.au
Coding * Design * Layout * Newton * Windows "Beyond the idea"

✶ SYN Floods, IP Spoofing, and what to do about it

"Fred Cohen" <fbcohen@california.sandia.gov>

Fri, 20 Sep 1996 09:14:27 -0700 (PDT)

Several years ago, several authors published details of a flaw in the design of TCP allowing denial of services via sending a SYN packet and not following up. In the last week or so, several magazines have published code for a SYN flood attack, and now many ISPs are going down because of their lack of defense and inability to trace the attacks to the sources.

I thought I would note that the CERT has now decided to advise all on the Internet to use the techniques against IP spoofing published some months ago in Network Security Magazine (Elsevier) in an article on IP spoofing (part of the "Internet Holes" series. This article was also published in the BoS mailing list (although they should not have done so because of copyright violation).

The basic defense is for the Internet community as a whole to refuse to route packets from known forged addresses. For example, we shouldn't be

routing packets from 0.0.0.0 and 255.255.255.255 or the IP addresses associated with internal-use-only IP ranges or - most importantly - packets from IP addresses not in the range appropriate to an incoming link. (If you service IP range 204.7.229.*, don't let inbound packets from that port with from IP addresses not in that range).

FC

🚨 More on portable electronics/airplanes ([RISKS-18.47](#))

Peter Ladkin <ladkin@TechFak.Uni-Bielefeld.DE>

Fri, 20 Sep 1996 08:49:52 +0200

Also see AWST Sep 9, p82. The RTCA is a non-profit organisation that evolves avionics and other electrical standards for aviation. It reports on RTCA Special Committee 177, formed in 1992 to consider just this potential problem.



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 18: Issue 49

Weds 25 September 1996

Contents

- [Minnesota State Senate candidate photo "mistake"?](#)
[PGN](#)
- [CIA disconnects home page after being hacked](#)
[PGN](#)
- [Cracker Bill Passes Senate](#)
[Edupage](#)
- [AOL Resumes Junk E-Mail Block, Settles Class Action Suit](#)
[Edupage](#)
- [Massachusetts welfare fraud investigators fired: tax-record misuse](#)
[Saul Tannenbaum](#)
- [Heart monitor software](#)
[Jim Garrison](#)
- [Automated toll collection test fails](#)
[George C. Kaplan](#)
- [Warning! NT 4.0 utility wipes system configuration](#)
[Alan Wexelblat](#)
- [Re: An unlosable casino game](#)
[Hal Lockhart](#)
- [FTC gets involved in P-trax debate](#)
[Bear R Giles](#)

- [Re: Lexis-Nexis P-Trak](#)
[Robert Ellis Smith](#)
 - [Re: Cracker Attack Paralyzes PANIX](#)
[Stephen Tihor](#)
 - [The RISKS of using "personal" info in authentication](#)
[Roger Moar](#)
 - [More ATM Risks](#)
[Roger Altena](#)
 - [Re: When is -32768 != -32767-1 ?](#)
[Bear Giles](#)
[Sidney Markowitz](#)
[Peter Jeremy](#)
[Mark Brader](#)
[Henry G. Baker](#)
[Erling Kristiansen](#)
 - [FWISC96 San Jose, CA](#)
[Mich Kabay](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ **Minnesota State Senate candidate photo "mistake"?**

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

Tue, 24 Sep 96 11:27:50 PDT

A photograph of Minnesota State Senate candidate John Derus appeared (without his name) on primary day in the **Star Tribune**, seemingly in connection with an article on a Philadelphia charity fraud case. Derus charges that the **Star Tribune** did this intentionally. (A lawyer for Derus cited a sworn statement from a caller who, upon complaining to the paper, was told that the use of the photograph ``may have been a personal act of vengeance by an individual employee for which the **Star Tribune** is not

responsible.' ' The *Star Tribune* had previously criticized Derus, and opposed him when he ran for mayor in Minneapolis in 1993.) The newspaper apologized and published an erratum the next day, claiming the mix-up was an innocent mistake resulting from a computerized system that assigns numbers to photos in which earlier photos had not been removed from the system.

This case could represent another RISKS example of how muddy the line can be between an innocent mistake and a malicious act that masquerades as an innocent mistake -- a topic that I discuss in my book, *Computer-Related Risks*. [Source: *San Francisco Chronicle*, 24 Sep 1996, A10.]

✶ CIA disconnects home page after being hacked

"Peter G. Neumann" <neumann@csl.sri.com>
Mon, 23 Sep 96 11:29:54 PDT

The CIA web site (<http://www.odci.gov/cia>) was penetrated by a group of Swedish hackers on 18 Sep 1996, causing the CIA to pull the plug the following day. The altered home page said, "Welcome to the Central Stupidity Agency." It also had valid links to Playboy and hacker netsites, and fictional links to ``news from space'' and ``nude girls''. Apparently, the Swedish intruders were protesting a Swedish court case against a group of youths who were caught breaking into computers in 1991. The CIA is presumably restoring its earlier web pages, which included spy-

agency press releases, speeches, and other publically available data, including CIA's World Fact Book -- all of course unclassified. [I just checked again before putting this issue out. The http address is still not working. The altered web-site content is reportedly at www.skeeve.net/cia . I did not check it.]

On the same day as the CIA shut its home page down, the Justice Department reopened its home page (<http://www.uswdoj.gov>), which had been hacked into the "Department of Injustice" in August. [Source: *San Francisco Chronicle*, 20 Sep 1996, A12]

[It will be interesting to see how these reminders (PANIX too) that the

our infrastructure is rather weak will play out. RISKS readers have of

course recognized the risks for many years, but Government policies have

not consistently reflected them. The flurry of activity might just

possibly encourage a change in attitudes toward security, encryption,

strong authentication, etc., and generally a ratcheting up the integrity

of the infrastructure -- although I am not holding my breath. However, a

possible partial administration relaxation in export controls is

reportedly being considered. Stay tuned. PGN]

✶ Cracker Bill Passes Senate (Edupage, 24 September 1996)

Edupage Editors <educom@elanor.oit.unc.edu>

Tue, 24 Sep 1996 22:17:37 -0400 (EDT)

A bill (S 982) that would make it easier to prosecute computer crimes passed the Senate last Friday, but its companion bill in the House (HR 4095) is not scheduled for any action. The National Information Infrastructure Act of 1996, sponsored by Senator Patrick Leahy (D-Vt.) would explicitly outlaw: interstate or foreign theft of information by computer; blackmail and threats against computer systems and networks; and unauthorized use of computer systems. Leahy says a Carnegie Mellon University report found that more than 12,000 computers were attacked in more than 2,400 incidents in 1995. The Computer Systems Policy Project reports that U.S. companies lost somewhere between \$2- and \$4-billion last year due to security breaches in computer systems. (BNA Daily Report for Executives 20 Sep 1996, A35; Edupage, 24 September 1996)

⚡ AOL Resumes Junk E-Mail Block, Settles Class Action Suit (24 Sep 1996)

Edupage Editors <educom@elanor.oit.unc.edu>
Tue, 24 Sep 1996 22:17:37 -0400 (EDT)

America Online has received permission from a federal appeals court in Philadelphia to resume its practice of blocking junk e-mail messages sent to its subscribers. Cyber Promotions Inc. had filed for and received an injunction earlier this month ordering AOL to end its practice of blocking unsolicited messages to its members from companies that

specialize in "junk e-mail" for promotional purposes. A related lawsuit is scheduled to go to trial in November. In a separate case, a judge in San Francisco tentatively approved a settlement to a class action suit brought by subscribers who claimed they were improperly charged for fractions of minutes that they didn't use. The settlement calls for refunds of \$2.95 for each \$300 in charges to former members. AOL's total payout could add up to \$700,000, \$200,000 more than was agreed to in the preliminary settlement. (*Wall Street Journal*, 23 Sep 1996; Edupage, 24 Sep 1996)

✶ Massachusetts welfare fraud investigators fired: tax-record misuse

Saul Tannenbaum <stannenb@emerald.tufts.edu>
Tue, 24 Sep 1996 20:23:28 -0400 (EDT)

>From *The Boston Globe*, Friday, 20 Sep 1996:
Gov. William F. Weld's aides yesterday fired two state welfare-fraud investigators who allegedly browsed the confidential tax records of some of Boston's most beloved sports heroes. [...] The pair left ``electronic fingerprints'' after calling up the records of Larry Bird, Ray Bourque and Drew Bledsoe, along with those of two of the investigators' former bosses. It is unclear why they did it, or whether they snooped through anyone else's files. [...] Last week, when they discovered the breach of computer security by someone at the Bureau of Special Investigation,

Department of
Revenue officials revoked the bureau's access to private tax
records. That
access has yet to be restored.

Saul Tannenbaum, Tufts University Computing and Communications
Services

stannenb@emerald.tufts.edu <http://www.tufts.edu/~stannenb>

⚡ Heart monitor software

Jim Garrison <jhg@mpd.tandem.com>

Tue, 24 Sep 1996 11:34:37 -0500

My wife works as a physical therapist in a local hospital, which
has several
sub-disciplines of PT including cardiac rehab. The cardiac
rehab department
has an exercise area in which patients can use stationary
bicycles while
connected to heart monitoring equipment, under the supervision
of a nurse.
The following "interesting" (from a RISKS perspective) incident
occurred
last week.

First, some background. According to my wife, the monitors have
CRTs and
display a standard EKG trace in a box, along with a large
numeric heart-rate
indicator. (Note: there are several different types of EKG
devices, the
most sensitive and discriminating being what is known a "twelve-
lead" EKG.
The monitor in use here is less sensitive, has fewer leads, and
is intended
for monitoring as opposed to diagnostic work).

When connecting a patient to the monitor, part of the procedure

involves setting a target heart rate. If the programmed rate is exceeded during exercise, the EKG trace turns red, but there is no audible alarm. There was at one time an audible alarm (on previous monitoring equipment) but it was considered more of a nuisance than a benefit, since it is normal to exceed the target by a few beats/minute for short periods of time and is not considered dangerous.

The monitoring software also has an option that can double the amount of EKG trace displayed by compressing the time axis. This operation mode is almost never used.

Now for the interesting part. A patient was attached to the monitor and began exercising. Somehow, unbeknownst to the nurse, the display was switched into compressed mode. When she glanced at the display, she saw what looked like a very high heart rate based on the spacing of the EKG peaks. She immediately went into "emergency mode", and set off a chain of events that led to starting an IV, calling the patient's doctor and preparing to administer a strong heart-rate-reducing drug. The doctor requested a 12-lead EKG for confirmation, at which point the error was discovered. Luckily, no drug had yet been administered. In declaring the emergency, the nurse had to miss or ignore a number of cues:

- 1) the numeric display still showed the correct heart rate (75)
- 2) the display had not changed color
- 3) the patient showed no signs of distress, remained totally calm, and repeatedly asserted he felt nothing out of the

ordinary.

While this is a fairly clear case of operator error, it's interesting to consider what the software designers could have done to make the error less likely:

1) Implement a progressive alarm system:

< 10 bpm over target	Yellow display, no alarm
10-20 bpm over target	Yellow display, single beep every ten seconds
> 20 bpm over target	Red display, continuous alarm

2) Provide a mode indication on the display when in compressed mode (maybe change the color of the EKG trace)

The first suggestion sounds good, but also might lead to complacency on the operator's part and excessive dependence on the alarm system itself, with more drastic consequences when IT fails. Sigh! Sometimes it seems like you just can't win.

The second suggestion just highlights the fact that man-tool interface "modality" is something people are not used to dealing with, as RISKS readers are well aware. (Cite five examples of tools in existence before 1950 with more than one interface mode; how about before 1900?)

Jim Garrison

Automated toll collection test fails

"George C. Kaplan" <gckaplan@cea.Berkeley.EDU>
Mon, 23 Sep 1996 22:01:47 -0700

An article in the 23 Sept. 1996 *San Francisco Chronicle* describes how Caltrans (California Dept. of Transportation) tested an automated toll collection system on the Carquinez Bridge, hoping to be able to use the system on all ten toll bridges in the state.

The test failed because the error rate was too high: Caltrans wants a 99.95% success rate (5 errors for every 10,000 tolls), but the system could do no better than 99.1%. Apparently the system had trouble recognizing different types of [multiwheel] vehicles in order to charge the correct toll.

The article didn't explain how the system is supposed to distinguish, say, a horse trailer from a big rig. A given vehicle may be in different toll classifications depending on what kind of trailer it's towing, so there must be some cues other than the encoding in the box carried on the vehicle.

There was no discussion of correct toll amounts charged to the wrong person, or what drivers would have to do to correct incorrect bills. Nor was there any mention of privacy issues (such as government tracking of individuals movements) that have appeared in previous RISKS discussions of automated toll collection.

George C. Kaplan gckaplan@cea.berkeley.edu 510-643-5651

Warning! NT 4.0 utility wipes system configuration

Graystreak <wex@tinbergen.media.mit.edu>

Mon, 23 Sep 1996 18:54:51 -0400

Forwarded-by: Logan Sanders <lsanders@chromatic.com>

NT users beware! Retail copies of both the Workstation and Server versions of Windows NT 4.0 shipped with an undocumented system-wiping utility. The file Rollback.exe erases key components of the system registry, disabling the operating system.

Microsoft Corp. officials say that once the file has been executed, the changes cannot be undone and require a complete reinstallation of the operating system. At least one incident of accidental erasure has occurred and Microsoft is mulling over how to inform customers of the problem.

This undocumented feature could do the most damage to NT4.0 Server users because it erases critical-security and user-account information. Without an up-to-date backup, network administrators will have to recreate all of the users' account and password profiles. Microsoft this week sent out an E-mail warning to its channel partners. It stated that after running the utility "the next thing the customer knows, they are staring at the set-up screen and are completely down."

Rollback.exe was designed to allow OEMs to test NT with their hardware and software configurations, and then return systems to their pre-installation state. The file is located in the support\deptools\I386\

directory of the NT CD-ROM and is not installed on the system by default. But the lack of any online documentation or escape route once the program has begun has put curious users at risk.

Microsoft officials say that more than 150,000 copies of NT Server 4.0 have been sold since its release in late July. Microsoft has posted an entry in its online Knowledgebase, but has not determined how it will notify customers and OEMs.

⚡ Re: An unlosable casino game ([RISKS-18.48](#))

Hal Lockhart <hal@platsol.com>
Wed, 25 Sep 1996 12:22:42 -0400

> just click on "BACK" ... and you undo your loss!

This reminds me of an bug I have seen in many computer-based gambling games:
the failure to check for negative bets. I always try this and it frequently works. You just make a negative bet and lose on purpose and the game subtracts your bet from your winnings!

Harold W. Lockhart Jr., Platinum Solutions Inc., 8 New England Executive Park
Burlington, MA 01803 USA (617)229-4980 X1202 hal@platsol.com

⚡ FTC gets involved in P-trax debate

Bear R Giles <bear@indra.com>

Tue, 24 Sep 1996 14:14:07 -0600 (MDT)

According to Reuter's, on Monday the Federal Trade Commission recommended Congress tighten consumer confidentiality laws to help stop credit fraud and identity fraud. The body of the article clearly referred to the current uproar over the Lexis-Nexis database, although not by name.

The article stated that in a letter to Sen. Richard Byran, D-Nev., the FTC stated that "fraud concerns outweighed the limited legitimate uses of this information for locating individuals." (quoting the article, not necessarily the letter.)

The letter further recommended that the Fair Credit Reporting Act be amended to require a legal release before a person's maiden name, Social Security number, prior addresses and date of birth can be released. I didn't see a reference to phone numbers, despite the perception by many people that "unlisted" phone numbers aren't readily available from such sources.

On an unrelated note, a brief note in the Saturday business section said that a three-judge appellate court overturned the lower courts injunction against AOL blocking spams from CyberPromotions. It's probably not a coincidence that the spam I received from them (non-AOL) on Monday highlights their new "block-proof, flame-proof" software.

Bear Giles bear@indra.com

✦ Re: Lexis-Nexis P-Trak ([RISKS-18.44](#))

Robert Ellis Smith <0005101719@mcimail.com>

Tue, 24 Sep 96 11:51 EST

The furor over the Lexis-Nexis database (which at first had anybody's Social Security numbers available to any strangers subscribing to the service) has caused a 180-degree turnaround in Congress, where anti-consumer amendments to the Fair Credit Reporting Act have been close to passage for the past four years. Congressional offices are getting lots of angry messages about Lexis-Nexis, because people realize that the source of the data is "header information" or "above-the-line information" at the top of our credit reports. The Federal Trade Commission over the past seven years has allowed this identifying information to be sold by credit bureaus without any protections of the Fair Credit Reporting Act (among other things, notice to the consumer).

Now, Congressional Republicans are actually thinking about protecting header information and reversing the FTC. They are thinking twice too about voting for anti-consumer amendments to the FCRA. People who are upset about Lexis-Nexis can have a real impact this week if they promptly convey their outrage to Members of Congress, especially their Senators and notably Sen. Richard H. Bryan, Democrat of Nevada, who might be supportive, fax 202/224-1867, and Sen. Alphonse D-Amato, Republican of New York and chair of the Banking Committee, who is probably not supportive, fax 202/224-5871.

Do it this week.

[P.S. If Americans - and most users of the Internet - were more upset about the demands for photo ID in order to board an airplane than about the Lexis-Nexis data base, the people in Washington would take note and reverse this pernicious invasion of privacy. Write the Federal Aviation Administration, the Department of Transportation, Members of Congress, and the news media.]

Robert Ellis Smith Privacy Journal, Providence RI 401/274-7861
5101719@mcimail.com

[I meant to insert a note earlier regarding the *pretense* that SSNs are hidden in P-Trak. If you have a CD-ROM version of the database, it is a very simple task to extract the SSNs. So much for "The SSNs are not accessible." PGN]

🔥 Re: Cracker Attack Paralyzes PANIX (Edupage, 12 Sep 1996)

Stephen Tihor <TIHOR@ACFcluster.NYU.EDU>

Sun, 22 Sep 1996 23:14:00 -0400 (EDT)

In general the PANIX attacks simply mark the point in the life of the Internet where zero-cost zero-security stops being a reasonable marketing point. If the net is to survive then it or the part that plans to become useful must add enough authentication and auditability to be able to track back and associate bad actions with the actors.

Once that is possible then normal time tested social mechanisms can be employed. The international nature of the internet means telecommunication standards and web of bilateral agreements and the law of the sea probably bracket the techniques that will work.

✶ The RISKS of using "personal" info in authentication

Roger Moar <rmoar@apertos0.csc.UVic.CA>

Tue, 24 Sep 1996 15:41:53 -0700 (PDT)

I was looking for some financial information, and came across the Barron's Online WWW site during my search. I tried to enter an area that is restricted to members, and was asked for my username and password. As I don't have an account, I clicked on OK, and was allowed to "FIND my password". I put in a silly username, and was greeted with:

"Hello John Doe. When you registered we asked you for your favorite color. Please enter your favorite color:"

(The names and passwords here are obviously fictitious.)

Naturally, I couldn't resist, and before I reached the end of the rainbow, I received:

"Congratulations! Hello John Doe. Your password is 3246297684".

I think the RISKS from this system are obvious. Repeated guesses of usernames brought up requests for the Mother's maiden name, date of birth,

or favorite color. Additionally, the usernames are easily guessed, any proper name seems to be taken as a username.

It's a nice way to give away information, but I'm not sure I would trust these people with my financial security...

Roger Moar -- rmoar@csr.uvic.ca | <http://apertos0.csc.uvic.ca/~rmoar>

⚡ More ATM Risks

Roger Altena <roger@mincom.com>

Wed, 25 Sep 1996 08:37:15 +1000

In my earlier days I was one of a team of ATM programmers. We had a machine in the office, and we tested the software by holding on to cards and envelopes, putting rubbish in the money bin, not taking receipts, and every other thing we could think of. It was a terrific job!

The operating system was specifically written for the ATM. It had instructions such as "get notes from hopper" and "present notes". If an instruction was used, the software automatically generated a mandatory error routine, which forced us to think of the correct action to take in each situation. It presented an error code with dozens of values for each instruction such as "less than the requested number of notes were presented", "some notes not taken", "all notes not taken", etc.

These days the software in ATMs seems to be written using generic languages,

and running on generic PCs. The risk is that by reducing costs, we take on the responsibility for thinking up each possible error ourselves, rather than leaving that job to a specialist who knows the hardware and its capabilities.

We also rely on a system where the hardware consists of an ATM built by one company, a PC by a second company, interface hardware from the ATM to the PC by a third company. Then the PC operating system is written by a fourth company, the ATM controlling software by a fifth, and so it goes on. Needless to say, the risks for misunderstanding and omission are multiplied manyfold.

Of course, this goes both ways. The hardware-specific software we used took up to 24 hours to generate, so the final software was full of patches applied through a hooked-in monitor. With modern PCs, a wide range of software development tools would greatly assist in producing stable and well structured code.

Roger Altena roger@mincom.com

✉ Re: When is -32768 != -32767-1 ? ([RISKS-18.48](#))

Bear Giles <bear@indra.com>
Tue, 24 Sep 1996 03:41:01 -0600 (MDT)

Numerous people have written me directly to point out that C defines

integers as a sequence of digits, and then uses unary negation for literal negative constants.

I wish to point out that both the Gnu C and HP/UX (the only compilers I've used for the past four years until the past few months) define

```
#define SHRT_MAX 32767
#define SHRT_MIN (-32768)
```

Many compilers are fairly intelligent about how they handle literal constants and expressions; perhaps this is how some (but not all) compilers can accept -32768 directly.

Bear Giles bear@indra.com

[A few comments follow. Similar overlapping comments were received

from many of you, including

Dik.Winter@cwil.nl (Dik T. Winter).

Andy Newman <andy@research.canon.com.au> ,

source@netcom.com (David Harmon),

thorinn@diku.dk (Lars Henrik Mathiesen),

"Kevin F. Quinn" <kfq@wormhole.comp.d.com>.

Jon Reeves <reeves@zk3.dec.com>, and

perhaps others unread whose subject line was merely "[RISKS-18.48](#)".

In addition, I excerpt starkly from some of the following replies. PGN]

✦ When is -32768 != -32767-1 ? (Giles, [RISKS-18.48](#))

Sidney Markowitz <sidney@research.apple.com>

Mon, 23 Sep 1996 12:55:28 -0700

[...] The problem is not with the Borland C compiler, which

performs
according to spec, but with Gnu Flex, which is generating C code
that does
not conform to the standard. Or perhaps the problem (and RISK)
is with the
type of thinking that expects people to see something like "(-
32767-1)" in a
large standards document and instantly understand all of the
nuances of the
standards committee's careful (and opaque) wording.

-- sidney markowitz <sidney@research.apple.com>

✉ Re: When is -32768 != -32767-1 ? (Giles, [RISKS-18.48](#))

Peter Jeremy <jeremyp@gsm01.alcatel.com.au>

Tue, 24 Sep 1996 08:39:08 +1000 (EST)

>Still, this situation is better than I would face when using a
personal copy
>of Microsoft Visual C++ 1.5. It limits SHRT_MIN to -32767.

This is a bit more dubious. Unless Microsoft have done
something strange to
two's-complement arithmetic, I'd say the definition was wrong,
since a short
can contain a value less than SHRT_MIN.

✉ Re: When is -32768 != -32767-1 ? (Giles, [Risks-18.48](#))

Mark Brader <msb@sq.com>

Wed, 25 Sep 96 02:16:45 EDT

[...] People who find C a RISKy language will like to cite this
quirk as

evidence. On the other hand, the absence of negative numerical constants has its advantages -- for instance, it frees the programmer from ever having to wonder whether things like -1 and -(1) might behave differently in some contexts.

[...] So here's another RISK -- a compiler where a warning **isn't** a warning. Instead it's 1/N of a fatal error, for some particular value of N. In my opinion that's a serious bug in the compiler.

Mark Brader, msb@sq.com, SoftQuad Inc., Toronto

🔥 When is -32768 != -32767-1 ? (Giles, [RISKS-18.48](#))

Henry G. Baker <hbaker@netcom.com>
Tue, 24 Sep 1996 07:32:37 -0700 (PDT)

So much for the 'science' part of 'computer science'...

There is a trivial and elegant solution to the problem of the asymmetry of 2's complement integers and how to input and convert them.

Low, James R. "A Short Note on Scanning Signed Integers". ACM Sigplan Notices 14, 1 (Jan. 1979), 55-56.

Briefly, instead of keeping the number as a `_positive_ integer`, you keep it as a `_negative_ integer` (which has a greater range), and then convert back if it is positive! In other words, "err on the Low side".

Pseudocode from Low's paper:

```
RESULT := 0;
while there are more digits, do
  RESULT := RESULT * 10 - current_digit;
if sign is positive, then RESULT := - RESULT
```

While we're on the subject, no one should be allowed near a numeric conversion routine until (s)he has read the following two papers:

Clinger, William D. "How to Read Floating Point Numbers Accurately". ACM Sigplan'90 Conference on Programming Language Design and Implementation, ACM Sigplan Notices 25, 6 (June 1990), 92-101.

Steele, Jr., Guy L., and White, Jon L. "How to Print Floating-Point Numbers Accurately". ACM Sigplan'90 Conference on Programming Language Design and Implementation, ACM Sigplan Notices 25, 6 (June 1990), 112-123.

Henry Baker www/ftp directory: ftp.netcom.com:/pub/hb/hbaker/home.html

✶ Re: When is -32768 != -32767-1 ? (Bear R Giles)

Erling Kristiansen <erling@wm.estec.esa.nl>
Wed, 25 Sep 1996 09:03:52 +0200 (MET DST)

This reminds me of a problem I had more than 10 years ago, using FORTRAN IV on an HP 1000. The comparison

```
IF (I .EQ. J)
```

results in FALSE when I and J are both -32768. This is because the HP 1000 has no COMPARE instruction, so, by necessity, the comparison is

done by SUBTRACTING one number from the other. Subtracting -32768 from -32768 (in 2's complement arithmetic) yields -32768, and an overflow condition which is not tested for by the generated code.

I was using this for comparing bit-patterns, and one of the patterns I was comparing against was Octal 100000 (= decimal -32768).

This confused me for a while!

🚀 FWISC96 San Jose, CA

Mich Kabay <75300.3232@CompuServe.COM>
24 Sep 96 12:25:14 EDT

NCSA is hosting its 2nd Firewall, Web & Internet Security Conference on Sept 30th and Oct 1st at the Red Lion Hotel, 2050 Gateway Place, San Jose, CA 95110. The exhibit hall is free and features most of the major developers of commercial firewall products. There will also be free vendor technical presentations open to exhibit hall visitors.

Details about the conference can be obtained by sending EMail to fwcon96west@ncsa.com or by visiting the NCSA web site at www.ncsa.com.

M. E. Kabay, Ph.D / Director of Education
National Computer Security Association



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 18: Issue 50

Thursday 3 October 1996

Contents

- [E-mail scam from "Global Communications"](#)
[PGN](#)
- [Vanity E-Mail Bugs College Administrators](#)
[Edupage via Dave Farber](#)
- [Rhode Island "Disgruntled employee" arrested for "e-mail virus"](#)
[Lee Rudolph](#)
- [ACLU Files Suit Against Georgia Internet Law](#)
[Edupage](#)
- [Clinton Okays Encryption Plan with Key Recovery System](#)
[Edupage](#)
- [Bellcore Warns Smart Cards Are Vulnerable](#)
[Edupage](#)
- [More side-effects from the Palo Alto power outage](#)
[PGN](#)
- [The new UK air traffic control system](#)
[Brian Randell](#)
- [Re: RISKS of temporary change-of-addresses](#)
[William K McFadden](#)
- [Two recent occurrences: ATM, change of postal address](#)
[Philip H. Smith](#)

- [Re: Postal change-of-address on-line](#)
[PGN](#)
 - [Watch your return address](#)
[Erann Gat](#)
 - [Queensland Police put Wanted Poster on the Web](#)
[Boyd Roberts](#)
 - [Getting scarier all the time](#)
[Erann Gat](#)
 - [Heart monitoring software](#)
[Bill Ragland](#)
[Tim Pietzcker](#)
[Steve Kilbane](#)
 - [More on Java security: see JavaSoft Forum](#)
[Marianne Mueller](#)
 - [Computerization and Controversy: Value Conflicts and Social Choices](#)
[PGN](#)
 - [Watch your return address](#)
[Erann Gat](#)
 - [Spring Forward, Fall Back -- but not just yet](#)
[Martin Minow](#)
 - [Airliner interference from a COMPAQ mouse, revisited](#)
[Paul Oldham](#)
 - [Advance Bank offers Internet Banking](#)
[Boyd Roberts](#)
 - [CFP Workshop on Formal Methods for Industrial Critical Systems](#)
[Diego Latella](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ E-mail scam from "Global Communications"

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

Thu, 3 Oct 96 9:00:34 PDT

Another e-mail scam has appeared, informing you as a would-be victim that you have "only 24 hours to settle your outstanding account" and

suggesting
that you can call an 809 number to avoid subsequent court
action. The call
goes to a Caribbean telephone company (apparently in Tortola in
the British
Virgin Islands) and costs you \$3 to \$5 (and presumably more if
you are dumb
enough to hang around for their strategy of putting you on hold
with a
sequence of creative recorded messages). The FROM: address
"Global
Communications"@demon.net is BOGUS. This is a cheaper variant
on a recent
809-900 pager scam, which costs you \$25 if you return the call.
[Source:
San Francisco Chronicle, 3 Oct 1996, A2.]

✶ Vanity E-Mail Bugs College Administrators

Dave Farber <farber@central.cis.upenn.edu>

Tue, 24 Sep 1996 21:34:23 -0400

A new e-mail service offered by New Century Technologies gives
customers an
e-mail address sporting a prestigious university domain name for
\$25 a year.
The customer, who must have a valid e-mail address somewhere
else, then
receives mail addressed to user@DukeU.com, or whatever school is
chosen. The
vanity address closely resembles the real thing, except it ends
in .com
instead of .edu. The universities aren't happy about the
impersonation:
"You can't assume people understand that the address isn't
affiliated with
the university somehow," says Florida State's director of Web
development. A
member of Georgia Tech's licensing committee is even more
adamant: "They

can't do that. People can't sell anything over the Internet and use our name without paying us royalties. We will fight this." (*Chronicle of Higher Education Academe Today*, 19 Sep 1996) [This evidently came from Edupage. PGN]

✂ Rhode Island "Disgruntled employee" arrested for "e-mail virus"

Lee Rudolph <lrudolph@panix.com>
Wed, 2 Oct 1996 06:55:00 -0400 (EDT)

Denise M. Johnson works for Aerotek (under subcontract from EDS) as a PC help-desk troubleshooter for Textron Corp. Textron is accusing her of planting a virus that caused them to lose all computer data for 15 hours beginning at 11 p.m. on 16 Sep 1996 and shutting down their system. She says she is innocent of the charge and attributes the allegation to ``office politics.'' She also noted that Textron's computers had been struggling with computer viruses for months and that the system crashed the same week she was accused of the crime. An investigation is in progress. ``The virus was already in the system,'' she said. [Source: Jonathan Saltzman, Computer Expert Faces Charge of Putting Virus in Textron's System, *Providence (R.I.) Journal-Bulletin*, 1 Oct 1996, page 1, PGN Abstracting]

✶ ACLU Files Suit Against Georgia Internet Law (Edupage, 26 Sep 1996)

Edupage Editors <educom@elanor.oit.unc.edu>

Thu, 26 Sep 1996 19:04:53 -0400 (EDT)

The American Civil Liberties Union has filed suit in federal district court in Georgia, challenging a new law that makes it illegal for organizations to "fraudulently misrepresent their Web site as that of another organization," says Representative Don Parsons, who sponsored the Georgia bill. The law also prohibits anonymously sending e-mail in some circumstances. Parsons' critic, Rep. Mitchell Kaye, says, "We've chosen to regulate free speech in the same manner that communist China, North Korea, Cuba and Singapore have. Legislators' lack of understanding has turned to fear. It has given Georgia a black eye and sent a message to the world -- that we don't understand and are inhospitable to technology." (*Wall Street Journal*, 25 Sep 1996, B1)

✶ Clinton Okays Encryption Plan with Key Recovery System (Edupage)

Edupage Editors <educom@elanor.oit.unc.edu>

Tue, 1 Oct 1996 20:49:33 -0400 (EDT)

Attempting to compromise with critics of its "key escrow" approach to data encryption, the Clinton Administration now plans to begin allowing U.S. computer companies to export software using powerful encryption

codes (or "keys") up to 56 bits long. However, the government will require those companies to develop, within two years, a "key recovery" system allowing U.S. law enforcement or anti-terrorist groups armed with a search warrant to get the key from the several third-party companies, each of which would hold one part of the key. IBM and some other large companies are supporting the plan, but other companies are expected to oppose it. The system will be successful only if the Administration can convince other countries to adopt the same kind of system. (*The New York Times*, 1 Oct 1996 C1; Edupage, 1 Oct 1996)

[There is a huge amount of netspace devoted to this topic in the past two days. It is likely to generate much discussion, although much of the basic arguments are made in earlier issues. I include the Edupage item to remind us to dig for it. PGN]

✶ Bellcore Warns Smart Cards Are Vulnerable (Edupage, 1 Oct 1996)

Edupage Editors <educom@elanor.oit.unc.edu>
Tue, 1 Oct 1996 20:49:33 -0400 (EDT)

Researchers at Bellcore have discovered that applying heat or radiation to a smart card's embedded chip can make it vulnerable to reverse engineering, allowing the data on the chips to be stolen. Michael Smith, director of the

Smart Card Forum, discounts the researchers' findings, however. He points out that smart card transactions require security passes by several systems, not just those on the card itself, and that exposing the card to heat or radioactivity would not result in repeatable faults, which would be needed for reverse engineering. "If what Bellcore says is right, that would mean you could bake 10 personal computers, turn them on, run a spreadsheet, and each one would show two plus two equaling five," says Smith. (*Investor's Business Daily*, 1 Oct 1996, A8)

[The researchers are Dan Boneh, Richard A. DeMillo, and Richard J. Lipton.

Their work is fascinating, and provides another wonderful reminder of how

difficult the security problem is. An article by John Markoff in *The New

York Times*, 26 Sep 1996, C1, seems more informative. The Smith quotes

are evidently inaccurate. Repeatable faults are not required. Baking

computers is not required. Stay tuned for the full article, which is due

out imminently. PGN]

⚡ More side-effects from the Palo Alto power outage

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

Mon, 30 Sep 96 15:09:33 PDT

One more effect of the 10 Aug 1996 west-coast power outage has come to light

in a letter from Sloane Citron of Menlo Park, published in the *Palo Alto

Weekly*, 18 Sep 1996. When the lights went out, a standby

generator kicked
in at the Cable Co-op transmitting point (the ``headend``).
Batteries kept
their phone service working, although their shared answering
service was
seriously overloaded. Finally, the batteries ran out on their
phone switch.
When power was restored, the cable system had to be brought back
on line,
although the knowledge of which customers were affected was not
available
because the phones were out. Meanwhile, back at the headend,
the circuit
board that normally scrambles the Playboy Channel was fried --
despite surge
protection. Sloane Citron's letter on behalf of Cable Co-op
apologized to
those cable viewers who were offended by having received the
Playboy Channel
unscrambled.

[Also known as raw video. I hope no lawyers tried on a surge
suit. PGN]

✶ The new UK air traffic control system

Brian Randell <Brian.Randell@newcastle.ac.uk>

Tue, 1 Oct 1996 23:14:56 +0100

The **Daily Telegraph** 1 Oct 1996 contains an article entitled:

"When Failure is Out of the Question" by Paul Forster

Quoting, admittedly **very** selectively, from the article (which
is approx.

600 words long):

National Air Traffic Services Ltd., part of the Civil Aviation
Authority, is

close to completing a new (pounds)300 million centre at Swanick . . . "It's all digital and probably the most advanced ATC setup anywhere," says Dr John Barrett, the Swanick project director, almost nonchalantly. "It's so complex I have difficulty in explaining it even to my board," he says. Throughout, safety is paramount. The whole system is made up of networked workstations rather than a central mainframe, so there is no single point of failure. . . . The system totals roughly two million lines of software, but like most software it is behind schedule and is still being debugged . . . Operations are not now due to begin until the winter of 1997 . . . "With ATC it's obvious that we simply have to remove all the faults in the code, and we are now working 24 hour a day, seven days a week," says Barrett. "Our over-arching requirement is that the system has to be completely safe."

How reassuring!

Brian Randell, Dept. of Computing Science, University of Newcastle,
Newcastle upon Tyne, NE1 7RU UK +44 191 222 7923 Brian.
Randell@newcastle.ac.uk

⚡ Re: RISKS of temporary change-of-addresses

William K McFadden <bill@tiktok.cse.tek.com>
26 Sep 1996 16:17:37 GMT

Simson Garfinkel related the problem he experienced with a temporary change of address. I had a similar problem when my ex-wife moved out and filed

permanent change-of-address forms for herself and our two-year-old son, of whom she had been awarded custody. Unfortunately, my son's name differs from mine only by middle initial.

For the last five years I have had nothing but trouble as a result, including my and my father's mail being delivered to my ex-wife's address; companies I do business with continually having the wrong address in their records, in spite of numerous attempts to correct it; and my voter registration being changed without my approval.

The risks of using change-of-address forms are many. For example, erroneous change-of-address data that continues to live on, long after it has been purged from post office systems; the inability or unwillingness of organizations to determine the age of change-of-address data, so that erroneous data continually displaces newer, corrected information; and governmental organizations changing registration records without direct, written notification from the party(ies) involved.

Bill McFadden Tektronix, Inc. P.O. Box 500 MS 50-350
Beaverton, OR 97077
bill.mcfadden@tek.com <http://www.rdrop.com/users/billmc>
(503) 627-6920

⚡ Two recent occurrences: ATM, change of postal address

703) 506-0500 <PHILS@RELAY.RELAY.COM (Philip H. Smith III,>
Thu, 03 Oct 96 09:12:15 EDT

A friend was at his grocery store, using his MOST card to buy about \$150.xx of groceries. He wanted \$30 cash, so he keyed in \$180.xx When he ran the card, it said "Daily limit exceeded". Which was wrong, as he'd not used the card at all that day.

He tried again without the extra \$30, and it worked.

He then went over to the ATM to try to get the \$30, and decided to get \$100 instead. It said "Daily limit exceeded". He tried \$30, and it said "Daily limit exceeded."

The next day, he of course called his bank to find out what was up. They looked at it, and found that *every one of the transactions* was recorded as having been successful -- so they'd deducted several hundred dollars more from his account than he'd received.

Not a friendly failure mode. He's still working on getting it straightened out.

The second item is from a web page, <<http://www.usps.gov/moversnet/coa.html>>.

It *looks* as if you can now forward anyone else's mail without ever having to set foot in a Post Office. A friend found this while looking for online forms, to save him time, as he *was* moving; he used this form, and it sent back e-mail "to confirm". This doesn't appear real secure, although not having tried to use this facility fraudulently, I can't be sure that there isn't some additional level of checking. (And for those who say "Hey, don't

spread FUD if you're not sure" -- well, the fact that I can't
tell is a
problem in and of itself, eh?)

...phsiii

✉ Re: Postal change-of-address on-line (Smith, [RISKS-18.50](#))

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

Thu, 3 Oct 96 8:03:31 PDT

This is an old problem whose electronic reemergence represents a serious potential escalation. The U.S. Postal Service folks in charge of on-lining the USPS have insisted that this problem would go away in the new system, but evidently it may have worsened. Perhaps we need to flood them with requests to DISABLE ENTIRELY the ability to change our own addresses electronically or by postcard, requiring in-person or certified requests (the USPS is now testing its entry into this business!), but it is likely to take a lot of requests before anyone will listen. By the way, the web page Philip Smith cites indicates that signing the change-of-address form certifies legitimacy of the request, and notes that anyone submitting false or inaccurate information is subject to punishment by fine or imprisonment. Given the ease of spoofing e-mail addresses, that is not likely to provide a sufficient disincentive. There have already been vastly too many scams (many untraceable) perpetrated using the old manual

approach. Caveant omnes.

✂ Watch your return address

Erann Gat <gat@aig.jpl.nasa.gov>

Fri, 27 Sep 1996 23:34:11 -0700 (PDT)

Today I got a message from David Jones (jones@random.org, names changed to protect the guilty) with whom I correspond regularly. David has a unique writing style and signature that would be impossible to reproduce by accident. It was only after I sent him a response that I noticed that this message was not from David after all, but from someone I'd never heard of, John Smith (smith@random.org).

Without thinking the situation through all the way I dashed off another note to John Smith asking him essentially who the hell he was and what he was doing impersonating my friend Dave.

Of course what happened was that Dave had been using a public Netscape browser that John Smith had at some earlier time configured for himself. David (who has a Ph.D. in nuclear physics, not a dumb guy) didn't know that you could even do that. He just assumed that the computer had some way of figuring out who you were and that you couldn't change it. The computer on his desk always does the Right Thing automagically, why wouldn't the one in the Library?

So John Smith, who has never heard of me or David Jones, now has

two very cryptic e-mail messages from me: my original reply to David, and my subsequent inquiry into John's identity. And David is wondering why I am taking so long to reply to his e-mail.

What is astounding about this mess is not only the sheer number of errors that had to be made in order to bring it about (four - John Smith not removing his personal e-mail configuration from the public computer, David Jones not reconfiguring the program before using it to send e-mail, my not checking the From address in the message, and my not thinking the situation through before sending my second reply) but also how utterly easy it was for all those mistakes to be made. In fact, for **all** these mistakes to occur is the **natural** evolution of events in the presence of Netscape running on a publically accessible machine. To eliminate **any** of these mistakes requires considerable effort and knowledge.

The risk: when you reply to an e-mail message you are **not** necessarily replying to the person who wrote it. You could be sending mail to a complete stranger through a completely innocent, and potentially very common, set of circumstances.

Erann Gat gat@jpl.nasa.gov gat@power.net

Queensland Police put Wanted Poster on the Web

Boyd Roberts <boyd@france3.fr>

Thu, 3 Oct 1996 10:17:45 +0200

After reading an article in the Sydney Morning Herald regarding the theft of a laptop from a shop and subsequent death of the shop's owner
[<http://www.smh.com.au/daily/national/961003-national6.html>] I checked out the Web page with the wanted poster for this crime, issued by the Queensland Police [<http://www.OntheNet.com.au/gcpolice/>].

It's certainly an inspired way to catch this guy, but the thing that strikes me is the RISK of the site being hacked [[RISKS 18.49](#): CIA disconnects home page after being hacked] or the DNS being spoofed and some random person's picture replacing the bad guy's. Not to mention the ease with which copies of such 'wanted posters' could be made.

I'm sure someone will point out that this sort of thing would be resolved when the bogus information was given to the Police. I am skeptical because it wouldn't be the first time that a wrong person/address mix up has occurred, sometimes with dire consequences.

⚡ Getting scarier all the time

Erann Gat <gat@aig.jpl.nasa.gov>
Mon, 30 Sep 1996 16:10:47 -0700 (PDT)

Today my doctor sent me to the HMO's lab to have some blood drawn. After jumping through the usual hoops (put the form in the slot, hand over the ID card, sign here, sign there) I was called in and seated in the

little room
with racks of empty vials on the wall. Twenty or so minutes
passed, which
seemed a little unusual, so I got up to find out what was
causing the delay.
I found the lab technician in another room looking at a computer
screen.
When I asked him what was going on he responded that he was
unfamiliar with
the procedure for one of the tests my doctor had ordered, and
was having
some trouble getting the instructions from the computer. Mo,
there was no
one else around whom he could ask.

Be afraid. Be very afraid. Erann Gat gat@jpl.nasa.gov
gat@power.net

✶ Re: Heart monitoring software (Garrison, [RISKS-18.49](#))

"Bill Ragland" <raglandb@smtplink.dis.anl.gov>

Thu, 26 Sep 96 11:53:35 CST

Jim Garrison's <jhg@mpd.tandem.com> description of an incident
with heart
monitor software in [RISKS-18.49](#) omitted to say whether either
the nurse or
doctor took a pulse before ordering a confirming ECG to
determine if the
heart monitor was inaccurate. If this was the case, it points
out another
risk not confined to computers, that of immediately attempting a
"high-tech"
solution to a problem when a "low tech" solution was at hand.
Often the
"low tech" solution offers results that are more intuitive and
easier to
interpret.

Bill Ragland

✉ Re: Heart monitoring software (Garrison, [RISKS-18.49](#))

Tim Pietzcker <pietzcke@ruf.uni-freiburg.de>

Thu, 3 Oct 1996 08:31:39 +0200 (MET DST)

I'm referring to the recent posting about the safety of medical monitoring devices. Or better, about the failure of people to read these properly.

First of all, as the poster said, they are no EKG (ECG if you're British) replacement. They are only used to diagnose disturbances of the heart's rhythm or frequency. Of course, if somebody switches the display to half speed, the spikes will still appear at the same rate which really is obvious (should be). Second, during an exercise situation it may be very difficult for the monitor to pick up the correct frequency because of all the artifacts generated by movement of the electrodes. On the other hand, the monitors are smarter than you might think from watching Arnold's latest movie "Eraser": No monitor I've seen would respond to disconnection of an electrode by showing a flatline EKG, so this "risk" is fictitious. What's more, no nurse or doctor would (should?) shock a patient who is moving about and protesting, only because his EKG is flatline. Moral: With all the machines we doctors get, we still have to think.

Tim

⚡ Re: Heart monitoring software (Garrison, [RISKS-18.49](#))

<Steve_Kilbane@cegelecproj.co.uk>

Thu, 26 Sep 1996 09:05:18 +0100

So it was the triggering condition that was wrong, not that the trigger caused an audible alarm. Sigh.

> She immediately went into "emergency mode", ...

This sounds quite good to me, actually, although not necessarily for the reasons implied. Ok, so it seems that a mistake was made, and was luckily detected before damage occurred. On the other hand, the nurse was acting as though a serious, time-critical problem existed, and moved to handle that problem, rather than wasting time checking the equipment - how often does RISKS carry tales of operators not believing that the situation was as bad as indicators claimed? Also, a sanity check was applied, **after** events were set in motion, but **before** damage was done. Personally, I would have thought a quick sanity-check with a stethoscope might have been appropriate, but I'm not in the medical profession, and don't know how effective it would have been.

steve

⚡ More on Java security: see <http://java.sun.com>

Marianne Mueller <mrm@Eng.Sun.COM>

Sat, 28 Sep 1996 12:06:58 -0700

RISKS readers are well aware of the difficulties inherent in trying to achieve strong security. JavaSoft is trying to increase general awareness of these problems relating to Java and related approaches, and has begun a series of forums that should be of considerable interest to many of you.

The first forum was on the topic of ActiveX and Java. The second forum is on the topic of security, and started running last week. You can find it at <http://java.sun.com/> . (Follow the link from the top level page.)

We're now hosting the second in the series of online Forums, and are inviting experts to comment on an opening statement from JavaSoft. We will publish statement and comments on our web page, and invite comments from the Internet community at large.

We are interested in feedback and comments. One thing we're hoping to do is to raise the level of commentary about security, because we feel that security is really an architectural issue, not a black-and-white-checkbox kind of issue. We recognize there are things that need to be fixed and we're working on that from an architectural or fundamental point of view.

Check out the Forum and send us your comments. We can't personally answer all the comments, but we plan to publish a subset of the feedback we get in a follow-up Forum.

Marianne Mueller mrm@eng.sun.com

✶ Computerization and Controversy: Value Conflicts and Social Choices

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

Mon, 30 Sep 96 14:46:30 PDT

Edited by Rob Kling

Computerization and Controversy: Value Conflicts and Social Choices

Second Edition

Academic Press, San Diego CA, 1996

The second edition of Rob Kling's book contains 78 articles with a wide variety of views representing a spectrum of authors, many of whom are familiar to long-time RISKS readers. The parts of the book are as follows:

- I. Heads Up! Mental Models for Traveling Through the Computer World
- II. The Dreams of Technological Utopianism
- III. The Economic, Cultural, and Organizational Dimensions of Computerization
- IV. Computerization and the Transformation of Work
- V. Social Relationships in Electronic Forums
- VI. Privacy and Social Control
- VII. System Safety and Social Vulnerability
- VIII. Ethical Perspectives and Professional Responsibilities for Information and Computer Science Professionals

There is much provocative thought in this collection, with a lot more than just a little something for everyone.

⚡ Spring Forward, Fall Back -- but not just yet

<minow@apple.com>

Tue, 1 Oct 1996 12:02:10 +0200

The biannual daylight savings time confusion began this weekend in Sweden.

When Sweden joined the EU (Common Market), it changed the fall changeover from the last weekend in September to the last weekend in October to conform with the rest of Europe.

Unfortunately, a few hundred thousand Windows '95 machines were not informed of the changeover and, followed pre-programmed instructions, switched on the old schedule.

This is, of course, one small example of a much more difficult problem:

there is no obvious way to pre-program daylight savings time changeover in a way that is sufficiently robust to withstand government intervention.

(My favorite example is Arizona, where federal land changes, but state land remains on mountain standard time year around.)

Martin Minow minow@apple.com

⚡ Airliner interference from a COMPAQ mouse, revisited (revisited!)

Paul Oldham <paul@bizanal.demon.co.uk>

Tue, 01 Oct 1996 09:57:32 GMT

In [RISKS-18.45](#) Mark Brader forwarded an article originally

posted by Dewayne Matthews in sci.aeronautics.airliners. In it Dewayne, commenting on a previous post that RFI interference with airliner systems is based on unsubstantiated anecdotal evidence goes on to give exactly the same sort of anecdote.

A valid reading of the episode is that the MD88's glass cockpit crashed for some unspecified reason and started to quietly re-boot. The pilot assumed RFI interference from PCs (he'd heard those anecdotes too) and got the only PC on board which was on turned off. Meanwhile the cockpit had completed its re-boot, entirely unrelated to the PC.

So yup, it's just another anecdote proving precisely nothing, expect perhaps that pilots listen to these stories too.

PS: meanwhile back in the real world of RFI interference I wonder if it's occurred to the airlines that many PDAs are actually all the time in standby mode and produce RFI. Just try putting an AM radio next to your PDA and listen.

Paul Oldham Milton, Cambridge <http://www.bizanal.demon.co.uk/paul/>

Advance Bank offers Internet Banking

Boyd Roberts <boyd@france3.fr>
Thu, 3 Oct 1996 18:21:53 +0200

I'm not really sure if these guys really know what they're doing, but the Advance Bank in Australia has offered Internet Banking:

<http://www.advance.com.au/advance/intbank/startup.htm>

It claims to use RSA and IDEA for encrypting the traffic between a PC based client and the server.

The RISKS? Where can I start?

They currently don't offer a Java version, but they say:

Will a Java Version be released?

Not for a while. While Advance Bank is often seen to be an "early leader" in new technology, Java is not yet a released product, nor are the security aspects finalised to our satisfaction. We'll keep a close eye on it, though.

"early leader?" Ahh... bleeding edge?

✶ CFP Workshop on Formal Methods for Industrial Critical Systems

Diego Latella <d.latella@cnuce.cnr.it>
Wed, 2 Oct 1996 12:51:20 +0200 (MET DST)

The Second International Workshop on Formal Methods for Industrial Critical Systems will take place in CESENA (Italy), 4-5 July 1997, close to Bologna (Italy) as a Satellite Workshop to the 24th International Colloquium on Automata, Languages, and Programming, sponsored by ERCIM Working

Group on

Formal Methods for Industrial Critical Systems, University of
Bologna, CNR /

Ist. CNUCE - Pisa, CNR / Ist. Elaborazione dell'Informazione,
Pisa

Dependable Computing Center.

More information can be obtained from

[http://fdt.cnuce.cnr.it:8080/Home/fm-ercim/WS/Cesena97/
workshop.html](http://fdt.cnuce.cnr.it:8080/Home/fm-ercim/WS/Cesena97/workshop.html)

STEERING COMMITTEE:

S. Gnesi - CNR/IEI - Pisa (IT)

D. Latella - CNR/CNUCE - Pisa (IT)

L. Simoncini - Univ. of Pisa and CNR/CNUCE - Pisa (IT)



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 18: Issue 51

Weds 9 October 1996

Contents

- [\\$850 Million Social Security Problem](#)
[Scott Lucero](#)
- ["ATMs chew up 400 bank cards"](#)
[Daniel P. B. Smith](#)
- [Crisps \(chips\), football \(soccer\) & the web](#)
[Geert Jan van Oldenborgh](#)
- [A Premature Comment on the Aeroperu Flight 603 B757 accident](#)
[Peter Ladkin](#)
- [You think this database anonymizes entries?](#)
[Identity withheld by request](#)
- [Re: RISKS of temporary change-of-addresses](#)
[Leonard Erickson](#)
- [Another mail-forwarding problem](#)
[Adrian Howard](#)
- [Risks of deferred ISDN charges](#)
[Bob Frankston](#)
- [Re: Queensland Police put Wanted Poster on the Web](#)
[Mark Eckenwiler](#)
- [Mailing list/vacation/autoresponder](#)
[Daniel P. B. Smith](#)

- [Re: USPS Mail Forwarding](#)
[Frank Caggiano](#)
[Jonathan I. Kamens](#)
 - [Re: politics and safety](#)
[Steven Philipson](#)
 - [Communications Unleashed - CPSR conference program](#)
[Susan Evoy](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✶ **\$850 Million Social Security Problem**

lucero <lucero@optec.army.mil>

Fri, 04 Oct 1996 11:11:15 EST

In the Daily Brief, the *Los Angeles Times* reported that, according to Social Security Administration officials, some 695,000 Social Security recipients have been underpaid since 1972, due to a computer program error.

- total unpaid benefits are estimated at \$850 million, with average amount per affected recipient of \$1,500.
- the SSA says about 400,000 of those affected have been identified and will be getting the back payments.

One RISK of latent bugs in financial systems is that dollars and interest really pile up after awhile.

Scott Lucero, U.S. Army OPTEC

[Note: [RISKS-16.67](#), 23 Dec 1994, had an item contributed by Mike Manos

from *Federal Computer Week, 21 Nov 1994, on the discovery of this problem, which at the time was estimated at \$478.5 million. That item

says that the problem occurred in 1978, when employers began reporting earnings annually rather than quarterly. The item I saw on 04 Oct 1996 said the software flaw was introduced in 1972. In any event, the problem was evidently first detected in 1994, as reported in [RISKS-16.67](#). PGN].

⚡ "ATMs chew up 400 bank cards"

"Daniel P. B. Smith" <dpbsmith@world.std.com>
Sat, 5 Oct 1996 13:39:06 -0400 (EDT)

The Boston Globe, 5 Oct 1996, p. B5:

> About 400 US Trust customers had their automated teller machine cards
> eaten Thursday night when the bank's linkup with the regional ATM network
> broke down for two hours. Bank officials said they still are trying to
> find out what went wrong.... Customers trying to use their ATM cards
> between 6:30 p.m. and 8:30 p.m. were told that their personal identification numbers had been keyed in incorrectly. When they tried it
> again, the machine ate their card. [A US trust spokesperson] said only
> US Trust customer's using another bank's ATM machine were affected.

You'd think "you have entered the wrong password" and "the network is down" would be distinguishable conditions with different error handling, wouldn't you?

Daniel P. B. Smith dpbsmith@world.std.com

✂ Crisps (chips), football (soccer) & the web

Geert Jan van Oldenborgh <gj@rulil0.LeidenUniv.nl>

Thu, 3 Oct 1996 23:20:13 +0200

Two weeks ago, one of the largest potato-cutters in the Netherlands started a competition. Building on the typical couch-potato's perceived expertise in football (soccer) they announced they would put a 'scorecard' into an unspecified proportion of their bags of crisps (chips). It has two scratchable pictures of a football game, without ball, and a superimposed grid. The idea was that the expert would guess where the ball was, verify that guess by scratching off the protective layer of that grid-square only, and claim fl 10 (~US\$ 6) when both were right.

However, the inevitable happened: two students set up a web site with the information gathered so far, and a request for anybody who had guessed right or wrong to share the information. Within two weeks the database had the correct ball position all 1445 pictures, and the crisp-fryer called off the competition, muttering things about unsportmanlike behaviour.

The RISK? Assuming knowledge does not spread is clearly not appropriate with the web around...

Geert Jan van Oldenborgh oldenbor@knmi.nl

✂ A Premature Comment on the Aeroperu Flight 603 B757 accident

Peter Ladkin <ladkin@TechFak.Uni-Bielefeld.DE>

Mon, 7 Oct 1996 21:05:59 +0200

On 2 Oct 1996, Aeroperu Flight 603, a Boeing B757, took off from Lima at

12.45am en route to Santiago, Chile, and disappeared from radar at 1.10am.

According to CNN, the pilot had reported mechanical problems, that he was

turning back, and had declared an emergency before radio and radar contact

was lost. I do not normally report details of accidents so early, for

reasons discussed recently in RISKS (Mills, 18.42; Dorsett, 18.43; Ladkin,

18.44; Mills, 18.45, Dorsett, 18.46) and am somewhat uncomfortable about

feeling a need to comment so soon on this case.

The Peruvian Transport Minister, Elsa Carrera de Escalante, declared

to The Times that "it seems there was a blockage in the computer system". According to CNN, she told a news conference that "it is not

the first time that one of these planes has had this kind of fault. We

have to find out why the computers went crazy". The Times reported the

story as `Computers Blamed...' and CNN as `Computer Failure Puzzling...' The Electronic Telegraph reported that Gen Juan Piperes,

fire chief of the Peruvian port of Callao, said: "The plane's whole

system completely failed."

I am thus concerned about a rumor starting that attributes the cause

of the crash to be a computer failure. It has not been so determined.

The information available so far to anyone is gleaned from the transcript of pilot/controller conversation, and radar plots. These, by themselves, are insufficient to determine the nature of the problems. Until the digital flight data recorder (DFDR) and cockpit voice recorder (CVR) are recovered and analysed, very little can be determined about the sequence of events leading to the accident.

The B757 was introduced into service in January 1983 [*] and flew until December 1995 with an unblemished safety record. There have been accidents on 20 December 1995 (near Cali, Colombia) and 6 February 1996 (near Puerto Plata, Dominican Republic), and now this one. In both of the previous accidents, pilot procedural errors, including errors in interacting with the flight management systems, played the decisive role. There were no technical failures, whether of structure or of flight management systems, involved in the Cali accident; the sole technical system failure in the Birgenair accident is (so far) presumed to have been caused by a blocked pitot tube. The B757 has three physically independent pitot-static systems, of which two seem to have been operating normally. It seems that normal procedures to cope with the single pitot-static failure were not followed by the Birgenair crew. The final report on the Puerto Plata accident is not yet published. If a computer failure 'caused' the Aeroperu crash, it would be the first time. There is no precedent for computer failure in a B757 accident, contrary to what Senora Carrera's statement would seem to suggest.

When the data from the CVR and DFDR are in, they might show that it would be worth questioning if the pilot's interaction with automated flight management may have contributed to the accident, as it did with both the previous accidents. Although this would be an HCI question, it's not a computer system failure per se. All sorts of hypothetical questions such as this may arise.

In any case, if computers were involved, it's exceptionally unlikely that they could be the sole cause, as I shall demonstrate. The B757 aircraft uses computer systems for displaying air data, for navigation, and for autopilot control and flight management. It does not use computers for flight control, which is achieved by conventional hydromechanical systems. Furthermore, the air data computer systems are backed up by conventional electromechanical 'standby' instruments of highly reliable design used for over half a century. The integrity of these physically-operated standby systems along with that of the physically-operated flight controls, as well as structural integrity, suffices to conduct safe flight in this airplane. From this fact, we may already draw some broad conclusions.

Let me thus divide the possible sequences of events into three. First, suppose normal control of the aircraft was lost. The B757 is conventionally controlled (not computer-controlled), and the air data systems have electromechanical backups. Therefore, in the event control was lost, either these backup systems would have had to fail also (in which case there would be a physical contributing factor), or

the pilot would have to have made ineffective use of these backup systems (in which case either inappropriate pilot action or some other cognitive confusion would also be a contributing factor), or the autopilot flew the aircraft into an out-of-control situation (as in the Birgenair accident), in which case the pilot's behavior in engaging and not disengaging the autopilot would be a factor, or the pilot would somehow otherwise have allowed control to be lost. No one has yet determined whether any of these situations occurred.

Second, if normal control was not lost, then either the aircraft must have suffered some form of structural failure in normal flight, which computers alone could not have been responsible for (structures can fail under normal control inputs if the aircraft is in an overspeed condition, but normally not otherwise); or the aircraft flew under control into the water (i.e., a CFIT, Controlled Flight Into Terrain, accident), in which case pilot behavior or engine failure must also have played a role.

These alternatives cover, grossly, all the possible scenarios. Since computers alone could not cause any of them, we may conclude that singling out computer failure of any kind cannot be the whole story. Since no one is able yet even to determine which of the above alternatives occurred (or one that I missed:-), it is certainly premature to attribute a cause of the accident.

More information on the accident, press reports, and the aircraft, as well as links to original sources and reports on the Cali and Puerto Plata accidents, may be found in my Compendium `Computer-Related

Incidents

and Accidents With Commercial Aircraft', available through
<http://www.techfak.uni-bielefeld.de/~ladkin/>

Peter Ladkin

[* 1983 is correct. This is a correction in the archive
copy. PGN]

⚡ You think this database anonymizes entries?

<[Identity withheld by request]>

Wed, 9 Oct 1996 11:38:58 PDT

Here's an interesting example of Info-War.

Many of us have seen and heard the television and radio
commercials for a
new in-home HIV test that is accurate, fast, and anonymous.

The test works as follows:

You buy the kit. Go home and follow the directions and obtain a
sample.

Mail the sample to the lab. In 3 days, call the lab and enter
in the

`secret' code and the results of the test performed on the
sample matching

your `secret' code will be revealed to you. The secret code is
used to

ensure anonymity so the user doesn't have to reveal their name.

Accurate? I believe so..

Fast? Three days is pretty fast..

Anonymous? Not at all!!! And here's why.

Whenever you call a 1-800 number, your phone number is captured

and forwarded to the company for billing purposes. It is also available to the PBX in the form of ANI which can be sent to the automated phone system that processes the request. In the HIV test scenario, the company that is called has a record of the calling phone number (ANI), and the requested 'secret' code. Since they already have the test results, the company is now able to match the phone number, which can be looked up, and the HIV status. In effect, the company is capable of covertly developing a database containing the names, addresses, phone number, and HIV status of the people who purchase and take the test.

Who would want this database?

Government, insurance companies, employers, you name it. Most health related information is considered confidential and will not be released by either the government nor the physicians. If someone had a 'secret' database that contained the HIV status of millions of people, then the interested organisations would have a discreet way of 'checking-out' potential clients, or employees.

⚡ Re: RISKS of temporary change-of-addresses (McFadden, [RISKS-18.50](#))

Leonard Erickson <shadow@krypton.rain.com>
Fri, 4 Oct 1996 23:33:29 PST

Try this one on for size.

I have the bad luck to have moved into an apartment where the previous tenant had the same last name. Other than that we have nothing in common as far as I can tell. I'm male, she was female. First names aren't at all alike.

But I still get her mail and have to be **very** careful about how I turn it over to the post office. The first time I just marked it "Not at this address, and it wasn't until a check didn't appear that I found out the post office had just blithely started bouncing my mail!

It's currently "handled" by my having had a talk with the carrier, and being careful to circle the first name **only** when writing not at this address...

>From comments made in this forum in the past, I'm not certain that the system the post office uses for tracking forwarding orders can deal with this properly. Anyone know for sure?

Oh yeah, to add insult to injury, I got a card from the previous tenant's dentist reminding him to come in for a checkup. I wrote "not at this address" on it and dropped it in the outgoing box. Several days later, it was back again. That's **really** stupid!

Leonard Erickson (aka Shadow) shadow@krypton.rain.com

Another mail-forwarding problem

Adrian Howard <adrianh@oneworld.co.uk>

Fri, 4 Oct 1996 11:50:48 +0100

Another mail-forwarding problem with a slightly different (and older) cause.

I've recently moved to flat numbered 03. Note that leading zero because, for various historical reasons I've yet to fathom, there is also a separate flat 3 at the same address.

I arranged mail forwarding from my previous address --- no prizes for guessing where the mail actually arrived.

After several phone calls, the operator at the post office finally realised that the software was stripping the leading zero as he typed it in... I now live at "flat zero three" as this seemed the only solution to the problem.

Since then I have encountered similar problems with various utility and delivery companies.

Risks: a variation of the old theme of making assumptions about the format of input data "nobody has an street name with more than 20 characters", "everybody has a middle initial", etc. Although in this case I think the person who came up with the foolish numbering system for the flats has to share some of the blame.

Adrian Howard. Head Techie. Victoria Real Ltd.

e. adrianh@oneworld.co.uk - v. +44 (0) 1273 774469 - f. +44 (0) 1273 779960

⚡ Risks of deferred ISDN charges

<Bob_Frankston@frankston.com>

Sat, 5 Oct 1996 15:13 -0400

This is in response to a query about why I received a year's worth of Long Distance charges all at once. The name of the carrier has been omitted to protect the very large long-distance carrier (or the remaining third). The original was sent all upper case, this is an OCR'd version.

DEAR ***

WHEN ISDN LINES ARE ESTABLISHED, A CARRIER FOR THE LONG DISTANCE PORTION OF THIS SERVICE IS CHOSEN EITHER BY CHOICE OR BY CHANCE. AT THIS TIME, THE LONG DISTANCE CARRIER IS SUPPOSE TO BE NOTIFIED THAT THEY HAVE BEEN CHOSEN TO PROVIDE THIS SERVICE BY THE CUSTOMER. OFTEN, NEITHER THE CUSTOMER NOR THE LOCAL TELEPHONE COMPANY INFORM THE LONG DISTANCE CARRIER THAT THEY HAVE BEEN PICKED. THIS RESULTS IN UNIDENTIFIED AND UNBILLED USAGE TO ACCUMULATE UNTIL THE USER CAN BE LOCATED AND DETERMINED BY THE LONG DISTANCE CARRIER.

THIS IS WHY YOU HAVE RECEIVED A BILL FROM *** FOR USAGE THAT IS ALMOST A YEAR OLD. SINCE THIS PARTICULAR SERVICE IS UNDER TARIFF (TARIFF F.C.C. NO.4), WE ARE REQUIRED BY LAW TO BACK BILL WHEN IT HAS BEEN DETERMINED WHO USED OUR SERVICE,

I HOPE THAT THIS EXPLANATION ANSWERS YOUR QUESTIONS REGARDING THE BILL THAT YOU HAVE RECEIVED. IF YOU HAVE ANY FURTHER QUESTIONS, PLEASE

GIVE US A CALL
AT .1-800-***-****

⚡ Re: Queensland Police put Wanted Poster on the Web (Roberts, R-18.50)

Mark Eckenwiler <eck@panix.com>
Fri, 4 Oct 1996 12:57:12 -0400 (EDT)

Of course, the FBI has had the Ten Most Wanted up in a web page here in the US for some time; see <http://www.fbi.gov/mostwant/tenlist.htm>

I wrote Director Freeh a letter many months ago pointing out that the FBI ought to a) digitally sign these mug shots and b) embed expiry dates, given the problems of forgery, ease-of-duplication/dissemination, and persistence. Risks include not only the inconvenience to wrongly apprehended persons, but also the cost to law enforcement of responding to citizen reports based on forged/stale Wanted notices.

I did not receive a reply.

⚡ Mailing list/vacation/autoresponder

"Daniel P. B. Smith" <dpbsmith@world.std.com>
Sun, 6 Oct 1996 11:13:47 -0400 (EDT)

So this guy goes on vacation, see, and he's on this mailing list that sends

out a 32K digest approximately daily, see, so when his autoreplier gets the mailing it sends back a chatty little personal note to the whole list, quoting the entire digest in full each time which, of course, creates a loop... and about the time someone gets THAT shut off, a very highly-placed honcho who is a _user-interface guru_ and _internet expert_ decides to send a chide-o-gram to this guy. Who's on vacation. Actually, it's his honeymoon, as he's mentioned. Repeatedly. So we _hope_ he isn't going to be hopping up every five minutes to check e-mail, right?

But accidentally, the highly-placed honcho sends this note to the whole list. Helpfully quoting the entire digest. In full.

Fortunately, this is a great mailing list and the back issues are well worth repeated rereading.

Yeah, it happens all the time, to all of us. And exactly how long have we been building e-mail software and mailing lists and using the network and reading and writing books about user interface design? Don't you sometimes think we're all too stupid to be trusted with anything important?

Daniel P. B. Smith dpbsmith@world.std.com

⚡ Re: USPS Mail Forwarding (Smith, [RISKS 18.50](#))

Frank Caggiano <caggiano@innet.com>
Fri, 04 Oct 1996 15:24:01 -0400

The web page

<http://www.usps.gov/moversnet/coa.html>

mentioned in [RISKS-18.50](#) for postal change of address does not send the change of address form electronically. (At least not as of 4 Oct). After reading the message in Risks, I thought I would try it out. Figuring that there would be a confirmation after filling out the form, I put in a change of address for myself. After entering information on a number of pages you are finally directed to print out the form and give it to your letter carrier or to mail it to your postmaster. There is some mention of their work on coming up with a secure system to allow the form to be filed via e-mail.

As for the suggestion that all change of addresses be done in person, I don't see how this would solve anything. A photo id would be required to confirm your identity (as a minimum) and we all know how easy it is to obtain a false one. Also any system is only as good as the people running it. On numerous occasions I have gone to the post office to pick up mail that they were holding for me and not once was I asked for ID (different offices, different clerks).

Frank Caggiano caggiano@innet.com <http://innet.com/~caggiano>

✉ Re: USPS Mail Forwarding (Smith, [RISKS 18.50](#))

"Jonathan I. Kamens" <jik@annex-1-slip-jik.cam.ov.com>

Fri, 4 Oct 1996 08:44:00 -0400

I see no risks from the WWW USPS Change of Address form that are not already present in the printed form available in any Post Office. In both cases, you never have to deal with a person or show any ID, and in both cases, submission of the form constitutes the claim that it is valid. Quite frankly, I don't see much of a "Risk to the Public in Computers and Related Systems" here -- if anything, it's simply a "Risk to the Public".

I will concede that since it's a lot easier to visit a WWW site and type in some information than it is to visit a Post Office, pick up a form, fill it out and mail it, the WWW form makes it easier for obnoxious people to submit false forwarding requests for other people. But I don't see that as a very big deal, especially because of the verification step outlined in the following paragraph.

Those of you who think that there isn't sufficient verification in the USPS mail-forwarding system should perhaps have read the Q&A About Mail Forwarding page available on the USPS WWW site. Quoting from it:

>How will the Postal Service verify that it received a Change of
>Address Order from me?

>

>The Postal Service will promptly mail you a confirmation letter to the
>address you are leaving, regardless of the date of your move.

(For
>your privacy, it will not mention what your new mail forwarding
>address will be.) Another confirmation letter will be sent to
you at

>your new address after the date of your move.

Yes, this does really happen -- I recently field a Change of Address order and did receive the two confirmation letters.

I assume that the USPS has sufficiently good "exception handling" that if you get a letter about a Change of Address Order you never filed and go to your Post Office and protest it, they can put a stop on the Change of Address. There is still some room for mischief, e.g., it's possible that some mail will be lost before you stop the forwarding, especially if someone is clever enough to file it while you are out of town or something, but the addition of this step still makes things a heck of a lot more secure than they were before.

I confess that I'm baffled about one thing.... When I put my mail on hold when I go out of town, and then go to the Post Office when I get back to pick it up, they require me to show ID before they'll give me the mail. I simply do not understand why they don't require people to show ID when submitting a Change of Address Order. The only explanation I can come up with is that right now, the minimal number of forged requests is outweighed by the increased convenience (and the less USPS-employee time consumed) of the current system; this presumably means that if forging Change of Address requests for other people ever becomes an "in" thing to do, the USPS is going to have to ditch the convenience and start requiring that forms be filed in person with ID and notarized by a USPS employee.

Jonathan Kamens | OpenVision Technologies, Inc. | jik@cam.
ov.com

✉ Re: politics and safety (Mills, [RISKS-18.45](#))

Steven Philipson <shp@wco.com>
Fri, 4 Oct 1996 16:26:40 -0700 (PDT)

In [RISKS-18.45](#), Dick Mills <dmills@albany.net> continued his argument on public speculation about the causes of airline disasters. He states:

>Mr. Dorsett expands on that theme when he says "It's a political world, not
>a technical one." I say no, never. Mixing demagoguery and science is
>irresponsible. It must never be tolerated.

That's a nice philosophy, but it has no connection to reality.

Public safety is **never** a technical matter. It is always and primarily political. If you are a technologist (as are most of us who read RISKS) then it is critical that you understand this **if** you want to have an effect on public policy. If there is no political force driving a public issue then nothing is done no matter how compelling the technical case. Technical changes are virtually never implemented unless someone has a political (or financial) motivation to do so.

Here's a case in point. In 1985 two friends of mine were killed while flying a light aircraft. When the details of the accident were

released it became obvious to me and several others that a major technical error was committed by the pilots. This was an error attributable to lack of knowledge/training. Unfortunately, the NTSB investigators on the case were also not familiar with the critical technical issue of the accident (dynamics of low-performance aircraft in mountain wave conditions) and omitted any mention of this error in the accident report. No recommendations have been issued which could help prevent additional accidents of this type, and they continue to occur with painful regularity

I have expended a significant amount of effort over the last 11 years in trying to get the NTSB and FAA to recognize the problem and to modify pilot and controller training such that accidents from this cause could be reduced or eliminated. There have been some encouraging results, but in the large the government has not moved.

The problem is **not** technical; the solution to the problem is well known. Rather, the problem is that there is not enough political force involved to motivate key government players. It likely will take either a major accident or the death of a prominent person before changes will be mandated.

In the meantime, public discussion of the issues is the **only** means available to disseminate this information and influence public safety. To that end, I have several web pages

<http://www.wco.com/~shp/waveforatc.html> and

<http://www.wco.com/~shp/speedtofly.html>

that are intended to inform people interested in the subject and keep the matter in the public eye. I also regularly speak on the subject at local venues and deliberately note the problem of political apathy on this matter. I am working on various political moves in an attempt to force the issue, but in the meantime all I can do is discuss the problem in public to the maximum extent possible.

Mr. Mills states: "Mixing demagoguery and science is irresponsible. It must never be tolerated." On the contrary. In this case and in others, mixing politics and technology is likely the *only* way in which public safety will be served. It is the only responsible course of action at my disposal.

Steve Philipson shp@wco.com

⚡ Communications Unleashed - CPSR conference program [RISKS-abridged]

Susan Evoy <sevoy@Sunnyside.COM>
Wed, 2 Oct 1996 11:39:02 -0700

COMPUTER PROFESSIONALS FOR SOCIAL RESPONSIBILITY
presents a conference on
COMMUNICATIONS UNLEASHED
What's At Stake? Who Benefits? How To Get Involved!

OCTOBER 19-20, 1996
Georgetown University, Washington, DC
Co-sponsored by the Communication, Culture, and Technology

program

of the Graduate School of Arts and Sciences at Georgetown University

Saturday sessions:

9:15 - 10:30 THE COMMUNICATIONS TSUNAMI
10:45 - 12:00 TOOLKITS FOR ACTIVISTS
1:30 - 2:45 THE INTERNET: COMMERCIALIZATION, GLOBALIZATION
AND GOVERNANCE
3:00 - 4:15 INFORMATION RIGHTS
4:30 - 5:45 COMPUTERS AND ELECTIONS: RISKS, RELIABILITY AND
REFORM
6:30 - 8:00 Dinner and presentation of the Norbert Wiener
Award to
Phil Zimmermann, inventor of PGP (Pretty Good Privacy)

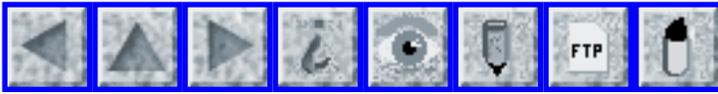
Sunday sessions:

9:15 - 10:30 Concurrent workshops
A. Using the Internet for progressive political
action
B. Internet legal issues
C. Broadcasting and mass media
10:45 - 12:00 Concurrent workshops
A. Communications access and the consumer
B. Media tactics and outreach
C. Civic networking

PM: CPSR ANNUAL MEETING (Attendance is free and open to the public)

FOR MORE INFORMATION ON THE CONFERENCE, CONTACT CPSR
at 415-322-3778, 703-739-9320 or cpsranmtg@cpsr.org or
<http://www.cpsr.org/home.html>
<http://www.georgetown.edu/grad/CCT>

Computer Professionals for Social Responsibility, P.O. Box 717,
Palo Alto CA
94302 Phone: (415) 322-3778 Fax: (415) 322-4748 evoy@cpsr.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 18: Issue 52

Saturday 12 October 1996

Contents

- [Rats take down Stanford power and Silicon Valley Internet service](#)
[PGN](#)
- [Punch-card ballots overturn primary election result](#)
[Dave Tarabar](#)
- [Pyramid schemes on the Internet](#)
[PGN](#)
- [Smartcard security and tampering vulnerabilities](#)
[Ross Anderson](#)
- [Are Laptops Risky at 30,000 Feet?](#)
[Edupage](#)
- ["Practical UNIX and Internet Security" by Garfinkel/Spafford](#)
[Rob Slade](#)
- [Novell and CC:Mail risk](#)
[John Colucci](#)
- [Maybe your secure Mac isn't as secure as you think](#)
[Carl Maniscalco](#)
- [Accidental denial-of-service to subscriber abuse@msn.com](#)
[Nick Rothwell](#)
- [ZIP Code Causes Misaddressing of Packages](#)
[Frank Markus](#)

- [``Return to sender''](#)
[Dik Winter](#)
 - [Re: Another mail-forwarding problem](#)
[Tony Lima](#)
 - [A Postmature Date on A Premature Comment](#)
[Peter Ladkin](#)
 - [CFP Computer Security Foundations Workshop 10](#)
[Simon N. Foley](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ Rats take down Stanford power and Silicon Valley Internet service

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

Sat, 12 Oct 1996 13:48:41 -0700

Two rats crawled through an underground cable conduit into a cabinet of power switching gear adjacent to the Stanford University cogeneration plant, and caused an explosion that cut off power to the Stanford area beginning around 7:30pm on Thursday evening, 10 Oct 1996, and continuing until 3:30pm Friday afternoon. The BBN Planet hub (Internet Point of Presence, or PoP) at the Stanford University Data Center remained in operation for a few hours on standby battery power, but then gave out around 9pm Thursday; it came back up around 4:30pm, an hour after Stanford restored power. To name just a few, Bay-Area BARNet users at Stanford, U.C. Berkeley, Apple, Sun, Hewlett-Packard, Lawrence Livermore (partially), and SRI were cut off from the Internet. The **Los Angeles Times** and **San Francisco Chronicle** on-line sites were also off the air. Because I had no Internet access

yesterday, I
held up [RISKS-18.52](#) -- thus enabling me to include this item
adding to our
RISKS archives collection of rodent-induced outages. (Long-time
readers
recall that SRI alone has contributed four fresh-fried squirrels
resulting
in power outages.) [Sources: On-line messages and a front-page
*San
Francisco Chronicle*, 12 Oct 1996 item]

Evidently, the horse is out of the BARNet, and the rats found
the weak lynx.
They sure put a ro-dent in the day for many BayAreans. Perhaps
your mouse
will click on a tale of its own. At any rate, this is just one
more saga in
the weak-link-in-the-infrastructure department. But I'm
surprised that
power-system technology has not found a way to develop rodent-
tolerant
circuits.

[With SysAdmins and others pacing the halls at SRI waiting for
whatever,

Doug Moran remarked that keeping around a few fresh-frozen
electrofried
rodents is allegedly standard practice for purveyors of power;
it is then
very easy to have a fallback alibi when no other cause can be
found.]

🔥 Punch-card ballots overturn primary election result

Dave Tarabar <dtarabar@systemsoft.com>

Thu, 10 Oct 1996 10:24:47 -0400

Punch-card ballots have been responsible for the uncertainty
about the

result of the Democratic Primary for the 10th Congressional District of Massachusetts.

The election was held on 17 Sep 1996. The official count was not released until two days later. Philip Johnston was said to have defeated William Delahunt by 266 votes out of 49,371 ballots cast. Delahunt called for a recount, citing some 1000 punch-card ballots that were counted as blanks by the mechanical vote counter. On 2 Oct, the results of the recount were announced that showed Johnston the winner by 175 ballots.

During the recount, the questioned ballots were examined by a human election official. The legal standard requires that the intent of the voter should govern the vote count. Thus if a ballot is not punched through, but is indented, then a vote should be counted.

Delahunt took the dispute to state court. A state court judge examined 956 ballots in chambers and ruled that only about 50 were actually blank. On 4 Oct, the judge declared Delahunt the winner by 108 votes. On 8 Oct, the Massachusetts Supreme Court upheld the decision, giving Delahunt less than a month to gear up for the general election.

It will be interesting to see what changes will be made for the general election. Punch-card ballots are used by 35 municipalities in Massachusetts (including mine). Hopefully there will be more education of voters to be sure that they completely punch out the perforation when they vote.

Dave Tarabar SystemSoft Corp. 2 Vision Drive Natick, MA 01760
508 647-2952 dtarabar@systemsoft.com

[This separates the "cent huit"[*] from the chaff (I'm punchy today)!

[* I seldom explain my obscurer puns, but this one is 108 au francais.] PGN]

✶ Pyramid schemes on the Internet

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

Thu, 10 Oct 96 13:03:51 PDT

Are you being flooded with spams and scams the way I have been? (With address variations on both my own account and RISKS, I often get at least FOUR copies of a given spam.)

The National Consumer League has issued a list of the top five types of Internet scams, based on complaints reported to Internet Fraud Watch. On top are (1) pyramid scams, such as Fortuna Alliance L.L.C. conning folks into paying \$250 to \$1750 by promising them \$5000 per month when others enrolled. Next in line are (2) bogus Internet-related services, (3) misleading equipment sellers, (4) fraudulent business opportunities, and (5) work-at-home offers. The Internet Fraud Watch can be reached in the U.S. at 1-800-876-7060 <nfic@internetMCI.com> <<http://www.fraud.org>>. [Source: *San Francisco Chronicle*, 10 Oct 1996, B3.]

Avoid a pyramid-life crisis. Don't be a sucker. Caveat emptor.

✦ **Smartcard security and tampering vulnerabilities ([RISKS-18.50](#))**

Ross Anderson <Ross.Anderson@cl.cam.ac.uk>

Thu, 10 Oct 1996 12:24:17 +0100

The smartcard security weakness [to interference phenomena] reported by Bellcore [Boneh/DeMillo/Lipton, noted in [RISKS-18.50](#)] is well-known in the TV-hacking community; power and clock glitches can be used to read out the memory contents of a number of smartcards. The typical modus operandi is to attack a loop in the card's software that reads out a series of memory addresses to the serial port. If a glitch can be found that causes the loop-variable decrement instruction to be wrongly decoded, then the entire contents of memory may be output.

Ross

[Stay tuned for a paper by Ross and Markus Kuhn of Purdue's COAST

Lab that they will present at the Usenix Electronic Commerce conference in November. Note that the A-K techniques for analyzing the

attack results are completely different from those of B-D-L, but the

triggering events can be similar. PGN]

✦ **Are Laptops Risky at 30,000 Feet? (Edupage, 10 Oct 1996)**

Edupage Editors <educom@elanor.oit.unc.edu>

Thu, 10 Oct 1996 16:35:06 -0400 (EDT)

A new report by RTCA Inc., a nonprofit group that advises the

airline industry, recommends tougher restrictions on the use of portable electronic devices during "all critical phases of flight." Some experts are even calling for a complete ban on all devices during flight. Currently, the Federal Aviation Administration leaves that decision up to individual airlines. In addition, the report recommends a total ban on all devices that transmit radio waves, such as a pager that automatically acknowledges receipt of a message by sending one back, or a laptop equipped with a wireless modem. Studies have shown that some of the strongest electromagnetic fields come from laptop computers, as the shielding that protects against unintended radio emissions tends to deteriorate over time. A laptop with a 90-Mhz microprocessor can leak radiation at that frequency as well as at higher, so-called harmonic frequencies, interfering with a plane's navigation and communications capabilities. (*Business Week*, 14 Oct 1996, p90)

✶ "Practical UNIX and Internet Security" by Garfinkel/Spafford

Rob Slade <roberts@mukluk.hq.decus.ca>
Thu, 10 Oct 1996 10:56:23 EST

BKPRUISC.RVW 960619

"Practical UNIX and Internet Security", Simson Garfinkel/Gene Spafford, 1996,
1-56592-148-8, U\$39.95/C\$56.95
%A Simson Garfinkel simsong@next.cambridge.ma.us simsong@gnu.ai.mit.edu

%A Gene Spafford spaf@cs.purdue.edu
%C 103 Morris Street, Suite A, Sebastopol, CA 95472
%D 1996
%G 1-56592-148-8
%I O'Reilly & Associates, Inc.
%O U\$39.95/C\$56.95 800-998-9938 707-829-0515 fax: 707-829-0104
nuts@ora.com
%P 1004
%T "Practical UNIX and Internet Security"

The title is certainly apt. This book is definitely practical, and if your job involves system security, at whatever level, this book belongs on your desk.

The expansion of the title is no mere attempt to gain market share: this edition is twice the size of the old one.

The book is well planned and comprehensive. While the emphasis and examples are from the UNIX operating system and Internet protocols, background information is given on related (and important) topics such as modems and physical security. The writing and examples are clear and understandable, and should present no problems to the intelligent novice, but the additional material ensures that there is value here even for the UNIX guru.

The six "parts" of the work (plus a set of appendices) present logical divisions of the topic. "Computer Security Basics" begins with an introductory chapter defining computer security, an operating system and UNIX. It continues with a discussion of policy and guideline considerations.

Part two deals with the responsibility of the user. The chapters deal with the defence of accounts and the protection of data through users and passwords; user accounts, "groups" and the "superuser"; and details of the

UNIX file

system. Part three looks at the system side of security, with attention to backups, integrity, auditing, malicious software, and physical and personnel security.

Part four covers communications aspects. This is highly important considering the strengths of UNIX in communications, the use of UNIX machines as bridges between other proprietary systems, and the participation of UNIX systems in the Internet. Chapters are devoted to modems, UUCP, TCP/IP, and Kerberos. Part five could be seen as an extension, dealing with advanced network security topics such as firewalls.

The sixth section begins to move away from strictly technical aspects, and starts to deal with your response to "security incidents". This may seem, to some, either irrelevant or defeatist. However, it points out an important attitude to have with respect to security: assume that, at some point, you are going to fail--and be prepared. The chapters here are no less practical than the foregoing, detailing the discovery of break-ins, denial of service attacks, and the (U.S.) legal aspects of security. (I appreciate the authors' forthrightness at this point: the chapter is entitled "Computer Security and U.S. Law", and doesn't assume one legal system fits all.)

A updating and expansion of a comprehensive and dependable classic in the security field

copyright Robert M. Slade, 1993, 1996 BKPRUISC.RVW 960619

Vancouver your Institute for Research into with your User Security Marcus	ROBERTS@decus.ca rslade@vanisl.decus.ca rslade@vcn.bc.ca Rob_Slade@mindlink.bc.ca Canada V7K 2G6	 	"Do you get guns with gun magazines? No. Do you get viruses virus magazines? Yes." - Kevin
--	--	-----------------------------------	--

🔥 Novell and CC:Mail risk

John Colucci <jcolucci@oak.kcsd.k12.pa.us>

Wed, 09 Oct 1996 21:18:47 -0700

Most folks know that on a Novell network the user is prompted to change their password every so often for security purposes. CC:Mail on the other hand is a password eternal system unless of course the user is not so irresponsible to never change it on their own volition. The Novell/CC:Mail double password system can be a fairly secure way to insure your mail account privacy. A trick to access the cc:mail accounts of all the local network users, bypassing the Novell login password follows. Login as you normally would using your own account. Go to the N: directory prompt and edit the hidden file "cc-mail.bat" to delete your user name. Save it and logout. Now login again and go to the n: prompt. This time when you type "cc-mail" you are presented with a universal login screen. Type in the users account name that you want to read. You are then asked for a password which in this case is usually a very easy guess. The usual last name, wife, dog,

kids, job title, nickname, works in the majority of cases. The sense of security that the initial Novell login password gives is enough to cause most people to pick really lame cc:mail passwords. What is REALLY funny is that the easiest accounts to hack at our company were the managers and supervisors accounts.

✶ **Maybe your secure Mac isn't as secure as you think**

Carl Maniscalco <caman@earthlink.net>

Thu, 10 Oct 1996 12:06:59 -0700

I recently downloaded a Macintosh shareware game from a reasonably trustworthy Web site. After playing it for a while, I decided it was worthwhile to pay the shareware fee. This particular software author (all names omitted to avoid unfairly painting anyone as a bad guy) included a small utility program that allows the user to fill out an on-screen form and print up an invoice for registration. Imagine my surprise when, upon launching this registration utility, I found my email address already listed in the appropriate field! , Many Mac Internet applications used with dial-up accounts either can (or in some cases, must) use a freeware control panel called ConfigPPP. I imagine that this is where the registration utility got my email address. ConfigPPP stores information about servers, user names and, if the user so chooses, account passwords in a central

location. These can be automatically polled by savvy Internet applications, thus making setup of each application simpler. Since the relevant computer is my home machine and used only by me, I had stored my PPP dollop account password in order to save a little time each time I log on.

When I printed up the shareware registration document, there were numerous lines of bar code printed at the bottom. These bar codes had what they ostensibly meant printed out in plain text beneath each line; however, there was no way I could confirm this was the information that the codes actually contained. For all I knew, they could easily contain my password. While I doubt very much that the shareware author in this case has done such a thing, it sure got me thinking about other potential security breaches. For instance, I imagine that it would be possible for a JAVA applet to poll ConfigPPP, pull out stored user names and passwords and send them off somewhere.

I have since deleted my password from ConfigPPP. Other Mac users may want to reconsider storing passwords on their "secure" computers as well.

--Carl Maniscalco, San Diego, CA--

⚡ Accidental denial-of-service to subscriber abuse@msn.com

Nick Rothwell <nick@cassiel.com>

Thu, 10 Oct 1996 10:52:06 +0000

This one is gleaned from reading news.admin.net-abuse.misc over the last week.

The Microsoft Network has a user with username "abuse" who now has a full mailbox. It's full of complaints by Internet users at large about junk mail from other users at msn.com.

Apart from the denial-of-service consequences for this user, it also means MSN's administrators are not getting abuse complaints (unless the poor user is dutifully forwarding them all).

Bottom line: an unfortunate interaction of a newly-established de-facto standard (abuse@domain.com for complaints about domain.com users) with an unlikely (although explainable) choice of username.

Nick Rothwell, CASSIEL <http://www.cassiel.com>

ZIP Code Causes Misaddressing of Packages

"Frank Markus" <fmarkus@pipeline.com>

Thu, 10 Oct 1996 08:04:22 -0400

Fire Island is a summer resort on a barrier beach off the south shore of Long Island. During the summer the various communities on the island have seasonal post offices that receive their mail from the mainland post office in Bay Shore (or Bayshore .. but that is another story), NY.

The seasonal post offices do not have individual ZIP codes or ZIP +4 extensions assigned to them. They are all assigned the same

11706 ZIP code
of the Bay Shore post office. That office sorts the mail
addressed to the
various Fire Island communities and sends it on to the
appropriate places.

Unfortunatly, when one tries to order something for
delivery to a
specific community on Fire Island, the "clever" software at the
mail order
vendor notices that the community specified is not the same as
that for the
ZIP code (Bay Shore) and helpfully changes it. Once the package
arrives in
Bay Shore, there is no way to determine to which of the several
Fire Island
communities it should be delivered. Even when I specify that my
community
must be manually entered and checked, it appears that the
software either
cannot be overridden or, if manually overridden once, wins in
the second
round.

I have taken to entering the name of my Fire Island
community as the
second line of my address after my street address much as one
would an
apartment number. This redundancy usually works but is at best
a clumsy
solution to the problem. And, of course, it is of no use
whatever to
seasonal renters who merely specify their name, address,
community and ZIP
code -- and are not in the phone book.

✶ ``Return to sender''

<Dik.Winter@cwil.nl>

Thu, 10 Oct 1996 04:09:22 +0200

We just had a special form of "return to sender". In order to obtain some of the benefits allotted to us according to Dutch law, we had to fill in some forms, put the forms in a pre-printed envelope, enter our address at the backside and put it in a mailbox. Much to our surprise the letter came back a few days later without any notice as to why it came back. Some study revealed the reason. The Dutch PTT prints in orange the "zip"-code as a bar-code on an envelope, in this case the code was printed on the backside, and apparently encoded our "zip"-code, so the person who did the "zip"-coding apparently had reversed the envelope after cancelling the stamp. Nobody in the remaining chain until delivery had seen what was happening.

This immediately created a new problem: how to get those forms to the institution where they were meant to go to on time? Time was short, and they only accept forms with the pre-printed envelopes and they had only a postbox address. Putting the envelope in the mailbox again might have many different results, return to sender again, delivered with postage due (the stamps were already canceled, and the institution does not accept letters that are not properly stamped), or whatever. Well, the letter was handed in person at the post office, they heavily crossed out the orange printed barcode, notices were put on the envelope saying "this is the sender" and "this is the addressee". And no, we have not yet received it back. We hope it was on time.

dik t. winter, cwi, kruislaan 413, 1098 sj amsterdam,
nederland, +31205924131
home: bovenover 215, 1025 jn amsterdam, nederland; <http://www.cwi.nl/~dik/>

✉ Re: Another mail-forwarding problem (Howard, [RISKS-18.51](#))

Tony Lima <tony.lima@toadhall.com>
Wed, 09 Oct 1996 22:19:00 -0700

Back in the days when I was giving dBASE seminars, I used the "stripped leading zero" as a reason to make fields for U.S. ZIP codes character type rather than numeric. At one such seminar in Boston (where 02215 is a common ZIP code), a participant noted that they'd sent their mailing list to a Texas company for processing and it had come back with four digit ZIP codes. Said participant now understood the problem better. Apparently some branches of the U.K. postal service don't.

tony.lima@toadhall.com (Tony Lima)

✉ A Postmature Date on A Premature Comment (Ladkin, [RISKS-18.51](#))

Peter Ladkin <ladkin@TechFak.Uni-Bielefeld.DE>
Thu, 10 Oct 1996 11:16:47 +0200

Steve Belle pointed out to me that the B757 was introduced in January 1983,

not 1993. Thanks to Steve for catching the inadvertent typo.
Yes, the B757
flew for nearly 13 years with its unblemished accident record.
Peter Ladkin

[I fixed the typo in the FTP.SRI.COM archive copy. PGN]

✶ CFP Computer Security Foundations Workshop 10

Simon N. Foley <simon@security.ucc.ie>
10 Oct 1996 13:36:11 +0000 (GMT)

Preliminary Call For Papers [Edited for RISKS]
10th IEEE Computer Security Foundations Workshop
June 10-12, 1997
Rockport, Massachusetts, USA
Sponsored by the IEEE Computer Society

This workshop series brings together researchers in computer science to examine foundational issues in computer security. We are interested both in papers that describe new results in the theories of computer security and in papers and panels that explore open questions and raise fundamental concerns about existing theories.

Possible topics include, but are not limited to:

access control authentication data and system
integrity
database security network security distributed systems
security
security protocols security models formal methods for
security
as well as foundational issues relating to other critical system
properties
and in emerging areas such as mobile computing and executable
content.

Submission deadline: 7 Feb 1997

For further information contact:

General Chair

Program Chair

Publications Chair

Jonathan Millen

Simon Foley

Joshua

Guttman

The MITRE Corporation
Corporation

Dept of Computer Science

The MITRE

Burlington Road,

University College

202

Burlington Road

Bedford, MA 01730-1420, USA

Cork, Ireland

Bedford, MA

01730-1420, USA

+1 617-271-3580

+353 21 902929

+1 617-

271-2654

jkm@mitre.org

s.foley@cs.ucc.ie

guttman@mitre.org

More online information at <URL:<http://www.jcompsec.mews.org/csfw.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 18: Issue 53

Thursday 17 October 1996

Contents

- [Stolen computer contains ophthalmology certification exam](#)
[PGN](#)
- [Computers miss \\$1.2M in ATM withdrawals](#)
[Jack Fenner](#)
- [Microsoft AGAIN distributes Macro Virus](#)
[Klaus Brunnstein](#)
- [Re: Rats take down Stanford and Silicon Valley Internet](#)
[Arthur P. Smith](#)
- [Health Info Database Misused](#)
[Duane Fickeisen](#)
- [Risks of not understanding the system](#)
[John Stewart](#)
- [RISKS of just having a name!](#)
[Nick Brown](#)
- [Telephone Switch Cutover Problem](#)
[Paul J. Mech](#)
- [Re: Maybe your secure Mac isn't as secure ...](#)
[Jon Callas](#)
- [Re: Another Mail-Forwarding](#)
[Tony Lima](#)

● [Risks of not including manual overrides: not a computer risk!](#)

[Jerry Leichter](#)

● [The Year-2000 Crisis](#)

[PGN](#)

● [Announcement: Year-2000 Software Crisis Conference](#)

[Hawkins Dale](#)

● [Info on RISKS \(comp.risks\)](#)

✂ **Stolen computer contains ophthalmology certification exam**

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

Wed, 16 Oct 1996 8:06:24 PDT

A laptop disappeared from a ``high-security'' suite in the San Francisco Palace Hotel while board examiners were out of the room for an hour in the morning of 15 Oct 1996. The laptop contained the questions for one segment of the national oral exam for doctors seeking ophthalmology certification. The hotel suite was reportedly accessible only by using one of six access mag-stripe cards, with the claim being made that hotel personnel could not possibly have had any access to the rooms. [Source: *San Francisco Chronicle*, 16 Oct 1996, A15]

[Now, why is it that cleaning personnel generally get in to hotel rooms for which you are told your unique registration-time-generated mag-stripe access code gives only you access? Ah, yes, RISKS readers probably won't believe that there could not have been any master-key cards, or emergency overrides, or other access modes such as creating a new access card from

the front desk, or somehow triggering the door release electronically

with an out-of-band signal! So, was this merely the theft of a \$5000

laptop? Or an attempt to eye the exam? (An-eye-for-an-eye-exam?) PGN]

✶ Computers miss \$1.2M in ATM withdrawals

Jack Fenner <jnf@pcisys.net>

Mon, 14 Oct 1996 21:03:39 -0600

The local paper here in Colorado Springs has had a series of articles about a "massive computer glitch" affecting 12,000 customers of a local credit union. Ent Federal Credit Union recently announced that it was about to subtract a total of \$1.2M from the accounts of its members because, for over a year, multiple identical ATM withdrawals on the same day were incorrectly processed. Only the first withdrawal was charged to the account. People without enough money in their accounts to cover what Ent decides they owe will be offered loans (at prevailing interest rates, of course). Ent blamed the problem on a "computer conversion" by the company that services its automatic teller transactions.

Naturally, some people are upset and are moving money out of their accounts.

The NCUA, which insures credit unions, is investigating, and (before they had a chance to actually investigate anything) gave Ent a clean bill of health and said it was in no danger of being closed. A variety of experts

have been interviewed by the newspaper, and all express astonishment that it took so long to be discovered (but curiously are not surprised that it happened in the first place). Ent says it has no choice but to collect the money because absorbing the loss "would wipe out nearly three months' profit". Ent is asking its internal auditor, Arthur Andersen, to "fully investigate the incident."

Also, newspapers have reported that many people reported the problem to Ent over the past months, and were ignored.

Besides the obvious risks of potentially uncollectable losses, disgruntled customers, and lost interest due to the time lag in charging accounts, there are a variety of other risks. Separate investigations by the NCUA and Arthur Andersen must be time consuming and expensive. Lawsuits are a possibility (if the computer is wrong about deducting multiple charges, why should we believe it about the charges in the first place?). Then there is the increased call for more federal oversight of credit unions in general and Ent in particular. Finally, there is the nightmare scenario: people decide that Ent is not safe enough for their money, and start a run on the credit union. Ent claims that while some money has moved out since the announcement, it is not a significant portion of their \$1B in assets. Even assuming that's true, I'd say it leaves them with no margin of error for future problems.

Jack Fenner, Colorado Springs

Microsoft AGAIN distributes Macro Virus

Klaus Brunnstein <brunnstein@rz.informatik.uni-hamburg.d400.de>

Mon, 14 Oct 1996 16:02:16 +0200

On ORBIT, a Swiss IT exhibition (held in Basel last week), Microsoft distributed a CD-ROM with a document (including German hotline numbers) infected with WAZZU.A Word Macro virus. Even when MS officials were made aware of this virus, the CD-ROM was continued to be distributed. At the same time, this infected document was also available for downloading from Microsofts Swiss Internet site, for several (at least 5) days after MS was warned.

MS experts at the exhibition said that this virus was "harmless". Indeed, WAZZU.A just interchanges (with probability of 1/5th) 2 randomly selected words in a document, and with a lesser probability, it inserts strings WAZZU.

Any Risk in Microsoft behaviour and attitude? "WAZZU" is a harmless string (does not delete anything :-), and random interchange of 2 words may even improve readability of texts :-). So, what risk?

Klaus Brunnstein (October 14,1996)

PS: For those with short memory: Microsoft was that company which released the first non-theoretical Word Macro virus, when it distributed, in July

1995, several CD-ROMs (dedicated to Windows 95 proliferation) with documents infected with Word.Macro.Concept (now .A). Until then, this was just a theoretical threat discussed first by Prof. Harold Highland back in 1989/1990. Since Microsoft`s pioneering work, almost 70 Word Macro viruses have been detected (plus one EXCEL and One AMIPRO Macro virus), some of which are "in-the-wild" primarily in the Anglo-Saxon Word World, but with fast development also in some non-Anglo-Saxon Word countries such as Taiwan and Germany :-)

[Check out the VIRUS-L Digest (listserv@lehigh.edu with the command "help virus-l"), which keeps up the WAZZU discussion (in 12 of the last 16 issues!). PGN]

⚡ Re: Rats take down Stanford power and Silicon Valley Internet service

"Arthur P. Smith" <apsmith@aps.org>
Sat, 12 Oct 1996 23:25:08 -0400 (EDT)

> But I'm surprised that power-system technology has not found a way to
> develop rodent-tolerant circuits.

I recently discussed this with a friend who is an engineer for LILCO (and well paid and qualified, thanks to our 18 cent/kwh rates). He pointed out that this was a very difficult problem due to the high voltages - you don't want ANYTHING in the neighborhood that provides a possible

electrical path
between the high voltage lines. The best thing to have as
insulation is
plain old air, but that leaves lots of room for little creatures
to get in
and mess things up. People have come up with lots of ideas for
fancy
enclosures, traps, noise-makers and the like to keep small
animals out, and
none of them have yet worked reliably for long. Anybody who can
figure this
one out will be saving the utility companies a lot of money (and
their
customers a lot of hassle)!

Arthur Smith (apsmith@aps.org)

[I was actually thinking about rat-tolerant systems along the
lines
of double-error-correcting, triple-error-detecting coding
systems,
where a system could for example tolerate two rats and detect
the simultaneous presence of a third by shutting down safely.
But I
was raticent to suggest it. PGN]

Health Info Database Misused

Duane Fickeisen <dfickeisen@Sunnyside.COM>

Thu, 10 Oct 1996 11:06:01 -0700

An AP story from Tampa Bay appearing in the Palo Alto Daily News
asserts
that a public health worker took a laptop and disks with
confidential lists
of people with AIDS and HIV home and to a gay bar to check out
the HIV
status of potential dates and offered to look up names of people
his
friends were interested in dating. One person asserted that he

had warned friends away from potential dates, telling them that their names were "on the list." Another claimed that people interested in dating him backed away after the health worker talked to them. The County Health Department has fired him, although he claims he did nothing wrong. The former health worker also owns and lives in a funeral home. The state had permitted such databases to be removed from offices and taken home until they changed their internal rules two weeks ago.

This raises anew questions about privacy and confidentiality of records, security, and misuse/abuse of information for personal and private gain. This ought to be raised up as an example of abuse in response to the announced plans for a national health information database.

Duane H. Fickeisen, Interim Director
Computer Professionals for Social Responsibility

⚡ Risks of not understanding the system

John Stewart <luigi@mars.dgrc.doc.ca>
Tue, 15 Oct 96 11:37:13 EDT

One day the accountants network printer failed. She needed some printouts from the financial computer in England. We were in The Netherlands. The "company" we worked for is based in Canada.

I called the maintainers of the financial system in London, and asked them

to re-route the account print queue to go to a different IP address. They could not, as that was considered a security risk, and nobody in London had the system privilege to make that change. Time zone differences meant that the people who could change it (in Canada) were still asleep.

So, I changed an ethernet address in the bootp table, rebooted a printer, and lo and behold, the accountants information came out on a printer in my office. She was happy. The people in London and Canada were not - I had broken their "security".

I also once made my manager the "head" of the organization, as she was requested by him to send out an e-mail in his name. It took me all of about 20 seconds to copy the passwd file, change his password, have her log in, etc, etc. She was amazed, and scared about the ease of such changes.

I could go on and on about the design issues of the network (and did, and was listened to, by the maintainers of the system - nice people!).

The RISK? I think that the exponential growth of networking usage has produced a whole range of uninformed "experts" who design systems and place unreasonable bounds on them.

It is not the experts fault - it takes time to gain experience, and that time is not available to them.

Needless to say, I no longer work for that organization.

John A. Stewart luigi@mars.dgrc.doc.ca

⚡ RISKS of just having a name!

"Nick BROWN" <Nick.BROWN@DCT.coe.fr>

14 Oct 1996 18:20:28 +0200

Bill McFadden (Re: [RISKS-18.50](#), RISKS of temporary change-of-addresses)

raises, perhaps inadvertently, an interesting point about people's names, describing his problems with his son's name differing from his own by just one initial.

Having been cursed at birth with three given names, I have become used over the years to appearing in lists several times, as N.Brown, N.J. Brown, N.J.L.Brown, etc etc. My wife has two given names, but has always used her second given name, perhaps fortunately for us because her first name (Nansi) begins with N too.

When our children were born, we used unambiguity of initials as one criterion for choosing their names (really !): manual systems have not served us well up to now, and computer systems do not have a good record of improving on the reliability of existing manual systems. Thus, our children both have exactly one given name (Alexander and Joanna respectively), neither of which begins with the same letter as ours.

In fact even "Alexander" is turning out to be a mistake: he is only ever called Alex, and I know he is in at least one (manual) database

under both
Alex and Alexander. This is partly because in France, most
people only ever
use one given name, and also because nicknames are relatively
rare. (In the
Netherlands, by contrast, it is not uncommon to have four given
names, and
be known (from birth) by a nickname which is unrelated to any of
one's given
names.)

When I visit the US, I find both manual and automated systems
quite unable
to cope with the idea of multiple "middle initials"; doubtless
my children
will have plenty of crashes when "middle initial = <empty>".
Somebody told
me that some Americans have middle initials that don't stand for
anything -
I wonder if their parents were anticipating software problems ?

Nick Brown, Strasbourg, France (Nick.Brown@dct.coe.fr)

⚡ Telephone Switch Cutover Problem

"Paul J. Mech" <paul@coil.com>
Sun, 13 Oct 1996 03:28:23 -0400

I thought this experience might be of interest to other RISKS
readers. In
the wee hours of Saturday morning (12 Oct 1996), I was ftp-ing
data from
around the world. My network-inspired happiness was marred by
my sudden
loss of the phone connection to my Internet provider. No
problem, these
things occasionally happen. However, the situation went to
annoying when my
modem announced "... your call could not be completed as
dialed ...".

After this condition persisted for thirty minutes, I contacted Ameritech. Residential Repair told me that they were told that this sort of behavior occurs when they are disconnecting a customer and forwarded me to Business Repair. Business Repair said that they couldn't comment on the situation because their computers were down. They did, however take my name and address and told me that they would call me back when they came back up. I left a couple of concerned messages on my provider's voice mail and decided to wait until morning.

By 10:00 AM Saturday, I had received no calls and the situation persisted. I pursued the same route, starting with Ameritech Residential Repair, and found things far less painful than the night shift had lead me to believe. At the time that I had been cut off, Ameritech had cut our exchange over to a brand spanking new switch. Our line checked out all right. Small Business Repair placed a call to the number that I was trying to reach and got through. Large Business Repair filed a trouble report and a technician called back shortly thereafter. As RISKS readers have no doubt concluded, the cutover apparently had a few unresolved bugs.

RISK 0 : Can you trust customer service?

By what I was first told, it seemed that my Internet provider was going out of business ... a scary thought, as I am not only pleased with this particular service, but I had to search quite a bit to find one who spoke *NIX this fluently.

RISK 1 : Emergencies

I am fairly savvy as to telephony problems, having spent several years programming for long distance resellers. Yet in the fog of the early AM, I obviously wasn't being too bright. What If someone had tried to place a call from our exchange to a doctor in my Internet provider's exchange? Would they have gotten through? Would they have though to call for operator assistance? How much time would they waste?

I'm not sure if there is any way I could have anticipated this, and I was no more than inconvenienced and slightly annoyed. But twenty four hours after the problem started, I'm back on line. Ftp is perking along happily in one window, and life is good again. I'm also glancing at a postcard that arrived this afternoon. It announces, in glowing terms, that Ameritech is going to install a new switch for our exchange on 12 Oct. It figures.

Paul J. Mech paul@coil.com pmech@freenet.columbus.oh.us

[⚡ Re: Maybe your secure Mac isn't as secure ... \(Maniscalco, RISKS-18.52\)](#)

Jon Callas <jon@worldbenders.com>
Mon, 14 Oct 1996 14:06:55 -0700

The "problem" is not with PPP. PPP does not store e-mail account names in its preferences file.

The problem almost certainly resides with something called "Internet Config." Internet Config is a database and API for storing information that Internet programs often need, oh, like your e-mail address. Your web browser wants that when it mails a page (or a message), your ftp program wants that to ease anonymous logins, and so on. Internet Config lets networking programs have a common database of information. It also allows programs like automatic shareware registration programs to know who you are, which is precisely what you saw.

Jon Callas Senior Scientist Apple Computer, Inc.

[Also noted by paul@ljl.com (Paul Robichaux) in a much longer message. PGN]

⚡ Re: Another Mail-Forwarding ([RISKS-18.52](#))

Tony Lima <tony.lima@toadhall.com>
Mon, 14 Oct 1996 09:45:00 -0700

[Several RISKS readers reminded Tony that
``branches of the U.K. postal service don't.''
should have read
``branches of the U.S. postal service don't.''
I fixed it in the ftp.sri.com archive copy. PGN]

⚡ Risks of not including manual overrides: not a computer risk!

Jerry Leichter <leichter@lrw.com>
Wed, 16 Oct 96 22:19:01 EDT

In [RISKS-18.47](#), William Hutchens reports his experiences at a hotel where an electronic keycard lock failed. Various "master keycards" also failed to open the door; "During the times I was left waiting in the hallway, I was half expecting the maintenance man to return with a sledgehammer". The door was eventually opened using a PC with a special interface. Mr. Hutchens says "I don't believe that it would be a problem to include a conventional mechanical keyway in the lock."

Just because a computer contributes to a problem, doesn't mean the computer *is* the problem. Just because there is no "mechanical override" doesn't mean there *should* have been one.

I, too, once found myself locked out of a hotel room by a failed lock. Repeated attempts to open the lock failed. My wife and I waited around in the hallway for quite some time as various attempts were made to get the lock to open. (The attempt that succeeded involved a ladder, a third floor window, and a hotel employee with a good head for heights.)

The only difference between our experience and that of Mr. Hutchens is that the lock in question was a traditional mechanical lock. Part of the mechanism broke, and literally fell off the door into the room. Without it, there was no way to open the door for the outside.

Should I complain about the lack of overrides for mechanical locks?

There would only be a valid complaint here if the electronic

keycard locks

failed as badly as Mr. Hutchens describes significantly more often than their mechanical brethren. I know of no evidence that this is the case. I do know that, in addition to my hotel experience, in the last year I found myself caught in a conference room at work when the (non-locking) door latch broke (the locksmith arrived shortly after I'd managed to remove the door from its hinges, a more elaborate job than it ought to have been); and I had to replace a broken lock on an external door at home after it, too, failed in a way that left the door "stuck shut". In that case, I had to literally smash the lock with a chisel in order to get the door open. Finally, while we were undergraduates (*so* many years ago, sigh), a friend got to call security to tell them he was locked *into* his room. Come again? You mean you lost your keys and are locked out, don't you? Well, no, the lock broke and I'm locked *in*.

Mechanical locks are not quite as reliable as Mr. Hutchens appears to believe, and when they do fail, the failures very often do require significant mechanical intervention - the guy with the sledgehammer - to get them open. That's essentially what the locksmith at the hotel I was staying at had to use to get the old lock out of the door; it's what he would have used to get in to the room if the third-floor-ladder trick hadn't worked. If most failures of keycard systems - even if more common than failures of mechanical systems - can be repaired by the simple use of a master card key,

I should think we're well ahead of the game.

-- Jerry

✶ The Year-2000 Crisis: a possible resource

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

Thu, 17 Oct 1996 17:15:24 PDT

I ran into Tom Reps this morning in San Francisco (where I had the pleasure of introducing Henry Petroski's wonderful keynote address to the ACM SIGSOFT Foundations of Software Engineering conference). Tom has been chartered by DARPA to make serious recommendations on the Year-2000 problem. I noted to him that a bunch of RISKS readers have offered me some possibly useful approaches, but indicated that it would be appropriate for those of you who believe you have something useful in this regard to contact Tom directly. I think he (and DARPA) would appreciate it. He can be reached at the Computer Sciences Department, University of Wisconsin-Madison, 1210 West Dayton Street, Madison, WI 53706-1685 1-608-262-2091, fax 1-608-262-9777 <reps@cs.wisc.edu> <<http://www.cs.wisc.edu/~reps/>>.

✶ Announcement: Year-2000 Software Crisis Conference

Hawkins Dale <hawkinsd@ttcus.com>

Thu, 17 Oct 1996 15:58:18 -0700

The Education Foundation of the Data Processing Management Association announces a conference on The Year 2000 Software Crisis

Information Systems professionals from the commercial, defense, and governmental sectors will share strategies and techniques for handling the coming potential disaster.

Date: 5--6 December 1996

Location: Alexandria, VA (the Radisson Plaza Hotel at Mark Center)

More information:

online info: <http://www.ttcus.com/y2k>

e-mail: ttchq@ttcus.com

voice: Hawkins Dale (310) 534-4871

Hawkins Dale
Technology Training Corporation
3420 Kashiwa St.
Torrance, CA 90505
voice: (310)-534-4871
fax: (310)-534-8585
alt fax: (310)-534-0743
e-mail: hawkinsd@ttcus.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 18: Issue 54

Monday 21 October 1996

Contents

- [A new attack on DES](#)
[Adi Shamir](#)
- ["Key Recovery" Replaces "Key Escrow" in Encryption Plan](#)
[Edupage](#)
- [Apology/Explanation for BBN-Planet outage](#)
[John Hight](#)
- [Snail causes Liechtenstein's cable TV system to fail](#)
[Henning Holtschneider](#)
- [Re: Rats take down Stanford ...](#)
[William Hugh Murray](#)
- [Re: Computers miss \\$1.2M in ATM withdrawals](#)
[William Hugh Murray](#)
- [Re: Health Info Database Misused](#)
[William Hugh Murray](#)
- [People Security versus Computer Security](#)
[Li Gong](#)
- [Info on RISKS \(comp.risks\)](#)

⚡ **A new attack on DES**

Shamir Adi <shamir@wisdom.weizmann.ac.il>

Fri, 18 Oct 1996 16:58:50 +0200

You have recently referred in RISKS [18.50, 18.52] to the ingenious new attack against public key cryptosystems developed at Bellcore. All the published information on the subject (including Bellcore's press release) stress that the attack is not applicable to secret key cryptosystems. Well, Eli Biham and I have just released a research announcement in which we show that an extension of the attack can, under the same realistic fault model, break almost any secret-key algorithm, including DES, multiple DES, IDEA, etc. The attack on DES was actually implemented on a PC, and it found the key by analysing fewer than 200 ciphertexts generated from unknown cleartexts.

Adi Shamir

= = = = =

Research announcement: A new cryptanalytic attack on DES

Eli Biham
Computer Science Dept.
The Technion
Israel

Adi Shamir
Applied Math Dept.
The Weizmann Institute
Israel

18 October 1996
(DRAFT)

In September 96, Boneh Demillo and Lipton from Bellcore announced an ingenious new type of cryptanalytic attack which received widespread attention (see, e.g., John Markoff's 9/26/96 article in the New

York Times).

Their full paper had not been published so far, but Bellcore's press release and the authors' FAQ (available at <http://www.bellcore.com/PRESS/ADVSR96/medadv.html>) specifically state that the attack is applicable only to public key cryptosystems such as RSA, and not to secret key algorithms such as the Data Encryption Standard (DES). According to Boneh, "The algorithm that we apply to the device's faulty computations works against the algebraic structure used in public key cryptography, and another algorithm will have to be devised to work against the nonalgebraic operations that are used in secret key techniques." In particular, the original Bellcore attack is based on specific algebraic properties of modular arithmetic, and cannot handle the complex bit manipulations which underly most secret key algorithms.

In this research announcement, we describe a related attack (which we call Differential Fault Analysis, or DFA), and show that it is applicable to almost any secret key cryptosystem proposed so far in the open literature. In particular, we have actually implemented DFA in the case of DES, and demonstrated that under the same hardware fault model used by the Bellcore researchers, we can extract the full DES key from a sealed tamperproof DES encryptor by analysing fewer than 200 ciphertexts generated from unknown cleartexts. The power of Differential Fault Analysis is demonstrated by the fact that even if DES is replaced by triple DES (whose 168 bits of key were assumed to make it practically invulnerable), essentially the

same attack
can break it with essentially the same number of given
ciphertexts.

We would like to gratefully acknowledge the pioneering
contribution of Boneh
Demillo and Lipton, whose ideas were the starting point of our
new attack.

In the rest of this research announcement, we provide a short
technical
summary of our practical implementation of Differential Fault
Analysis of
DES. Similar attacks against a large number of other secret key
cryptosystems
will be described in the full version of our paper.

TECHNICAL DETAILS OF THE ATTACK

The attack follows the Bellcore fundamental assumption that by
exposing a
sealed tamperproof device such as a smart card to certain
physical effects
(e.g., ionizing or microwave radiation), one can induce with
reasonable
probability a fault at a random bit location in one of the
registers at some
random intermediate stage in the cryptographic computation. Both
the bit
location and the round number are unknown to the attacker.

We further assume that the attacker is in physical possession of
the
tamperproof device, so that he can repeat the experiment with
the same
cleartext and key but without applying the external physical
effects. As a
result, he obtains two ciphertexts derived from the same
(unknown) cleartext
and key, where one of the ciphertexts is correct and the other
is the result
of a computation corrupted by a single bit error during the
computation. For

the sake of simplicity, we assume that one bit of the right half of the data in one of the 16 rounds of DES is flipped from 0 to 1 or vice versa, and that both the bit position and the round number are uniformly distributed.

In the first step of the attack we identify the round in which the fault occurred. This identification is very simple and effective: If the fault occurred in the right half of round 16, then only one bit in the right half of the ciphertext (before the final permutation) differs between the two ciphertexts. The left half of the ciphertext can differ only in output bits of the S box (or two S boxes) to which this single bit enters, and the difference must be related to non-zero entries in the difference distribution tables of these S boxes. In such a case, we can guess the six key bit of each such S box in the last round, and discard any value which disagree with the expected differences of these S boxes (e.g., differential cryptanalysis). On average, about four possible 6-bit values of the key remain for each active S box.

If the faults occur in round 15, we can gain information on the key bits entering more than two S boxes in the last round: the difference of the right half of the ciphertext equals the output difference of the F function of round 15. We guess the single bit fault in round 15, and verify whether it can cause the expected output difference, and also verify whether the difference of the right half of the ciphertext can cause the expected difference in the output of the F function in the last round (e.

g., the difference of the left half of the ciphertext XOR the fault). If successful, we can discard possible key values in the last round, according to the expected differences. We can also analyse the faults in the 14'th round in a similar way. We use counting methods in order to find the key. In this case, we count for each S box separately, and increase the counter by one for any pair which suggest the six-bit key value by at least one of its possible faults in either the 14'th, 15'th, or 16'th round.

We have implemented this attack on a personal computer. Our analysis program found the whole last subkey given less than 200 ciphertexts, with random single-faults in all the rounds.

This attack finds the last subkey. Once this subkey is known, we can proceed in two ways: We can use the fact that this subkey contains 48 out of the 56 key bits in order to guess the missing 8 bits in all the possible $2^8=256$ ways. Alternatively, we can use our knowledge of the last subkey to peel up the last round (and remove faults that we already identified), and analyse the preceding rounds with the same data using the same attack. This latter approach makes it possible to attack triple DES (with 168 bit keys), or DES with independent subkeys (with 768 bit keys).

This attack still works even with more general assumptions on the fault locations, such as faults inside the function F, or even faults in the key scheduling algorithm. We also expect that faults in round 13 (or even prior to round 13) might be useful for the analysis, thus reducing the

number of
required ciphertext for the full analysis.

OTHER VULNERABLE CIPHERS

Differential Fault Analysis can break many additional secret key cryptosystems, including IDEA, RC5 and Feal. Some ciphers, such as Khufu, Khafre and Blowfish compute their S boxes from the key material. In such ciphers, it may be even possible to extract the S boxes themselves, and the keys, using the techniques of Differential Fault Analysis. Differential Fault Analysis can also be applied against stream ciphers, but the implementation might differ by some technical details from the implementation described above.

✶ "Key Recovery" Replaces "Key Escrow" in Encryption Plan (Edupage)

Edupage Editors <educom@elanor.oit.unc.edu>
Fri, 18 Oct 1996 09:21:58 -0400 (EDT)

The latest government proposal for encryption software controls touts a new approach called "key recovery." This provision would allow law enforcement officials to rebuild, or "recover" the mathematical key to encoded messages with the help of third-party code-breakers. The new policy reflects suggestions made in a National Research Council report released earlier this year. Under the Clinton plan, encryption keys would be expanded from 40 bits to 56 bits in products to be exported, provided the company agrees to

the key recovery process. In addition, authority to issue licenses for overseas sales of such products would move from the State Department, where they're handled as "munitions," over to the Commerce Department. The Business Software Alliance, however, is still not completely happy with the compromise. "We expect to go back to Congress," says a BSA spokeswoman.

"Although the announcement was clearly a step in the right direction, it's not at all what the industry was looking for in its entirety." (*Investor's Business Daily* 17 Oct 1996 A4; Edupage 17 October 1996)

⚡ Apology/Explanation for BBN-Planet outage

John Hight <hight@std.sri.com>
Fri, 18 Oct 1996 10:15:41 -0700

Here's the official apology and explanation of the BBN-Planet outage last week. I'm a little put off by Paul Gudonis's offer for credit for two days of service in his last paragraph. As everyone knows, the cost of not being able to do business is vastly greater than the cost of keeping up our single T1 line here at SRI.

John Hight SRI International hight@sri.com

>Date: Wed, 16 Oct 1996 16:26:29 -0500
>To: affected-sites@bbnplanet.com
>From: Paul Gudonis <pgudonis@bbnplanet.com>
>Subject: Palo Alto Power Outage

>

>This letter is to our customer administrative and technical contacts

>who were affected by the outage last week at BBN Planet's Palo Alto
>POP. I know how detrimental even a short outage of Internet service
>is to your business; I have spoken to many of you and understand how
>drastic an impact the lengthy outage on Friday had. I want to
>communicate what we know about the cause of the outage and what steps
>we took and are taking.
>
>BBN Planet's Palo Alto POP is collocated at Stanford University's data
>center. This facility, in addition to handling the University's data
>systems, hosts systems for the Stanford University Hospital. Stanford
>has redundant power systems, drawing on both Stanford's co-generation
>facility and PG&E power. Stanford has had continuous power at this
>facility for over 10 years, including during earthquakes and during
>the brownout that the western region experienced in August.
>
>The equipment that switches between these power sources failed last
>Thursday at 7 pm PDT. Battery backup allowed us to continue powering
>equipment through 9 pm PDT. Stanford's power was restored at 12:30 am
>PDT Friday. BBN restored service to the majority of customers affected
>by 1:20 PDT. Stanford's power failed again at 6 am PDT. Due to the
>previous outage, the backup batteries were not fully recharged at this
>point and BBN Planet's power was lost.
>
>Two backup generators were ordered and in place by 2 pm PDT. One
>generator was required for the cooling systems, the second for the POP

>equipment. When the generators started running, one failed.
To avoid
>further failures, two additional generators were ordered and
one was
>in place by 3:30 pm PDT. As the second generator was being
started
>up, main power was restored to Stanford at 4:30. Over the next
hour,
>the temperature in the POP was stabilized, the POP equipment was
>restarted and service restored to customers.
>
>>From the time the first outage occurred, BBN Planet field
service staff
>remained on site. I was personally at the Palo Alto facility
to ensure
>that our local staff had any resources -- internal or external
--
>required to restore service to you as quickly as possible. At
both
>headquarters and our Western Region offices, additional staff
were
>recruited to personally call each customer and inform them of
our
>plans. Our 800 632 7638 line was updated as new information was
>available.
>
>I am proud of dedication the BBN Planet staff showed in
addressing
>customer concerns and striving to restore service as fast as
possible.
>However, none of us are satisfied with our performance.
Although the
>redundant power at Stanford had performed with 100% reliability
for
>the last 10 years, we are taking additional steps to ensure
that power
>outages do not impact our customers. The generators will be
kept on
>site to avoid further outages until they are replaced with a
permanent
>generator. They are being manned 7 x 24 to ensure we can start
them
>up before the batteries are exhausted.

>
>While BBN Planet's staff did its best to contact customers, we
were
>not able to call as often or as early as we, or you, would
like. We
>will have an operational Emergency Broadcast System in place in
>December that will allow us to contact all affected customers
within a
>few minutes. We'll update you as this service comes on line.
>
>We have also made substantial investments in our network
>infrastructure to deliver the service quality that you expect.
In the
>last six months, we deployed a high-capacity national backbone
with
>redundant facilities, expanded our server operations, and
implemented
>new systems for customer support. We are continuing to install
more
>capacity, more redundancy, and new systems to meet your evolving
>needs. We'll keep you informed of these improvements.
>
>We are automatically issuing credits for two days of service to
all
>customers who lost service due to the Palo Alto power failure.
We
>have made significant investments and continue to strive to be
the
>most reliable Internet Service Provider. After this incident,
we have
>a ways to go to regain your confidence, but will make every
effort to
>do so.
>
>Regards,
>
>
>Paul R. Gudonis
>President
>BBN Planet

🚀 Snail causes Liechtenstein's cable TV system to fail

Henning Holtschneider <hh@hhome.farside.net>

Fri, 18 Oct 1996 22:30:16 +0200 (MET DST)

As far as I can see from the archives, this is the slowest animal ever to make it into the RISKS gallery of "rodent"-caused outages ;-)

According to a local newspaper, Soccer fans in Liechtenstein were unable to watch the last couple of minutes of a soccer match between the French team of Auxerre and Switzerland's Zuerich Grasshoppers when a snail crawled into a socket. The resulting short-circuit caused the entire cable TV network of Liechtenstein to fail.

Henning Holtschneider * Bauernkamp 41 * 44339 Dortmund * Germany
hh@hhome.farside.net

[Don't forget the GraceHopper bug, although it had the potential for higher speed. PGN]

🚀 Re: Rats take down Stanford ... ([RISKS-18.53](#))

William Hugh Murray <0003158580@mcimail.com>

Fri, 18 Oct 96 11:03 EST

PGN's request for redundancy brings to mind the story of the infrastructure computer center in Trumbull, Connecticut. It is an old story but bears repeating.

Seems that a squirrel got into a transformer and brought down the external

power supply. The UPS kicked in, engine generators came on line, and the center operated in this mode for about an hour and a half. At the end of that time the external power was restored. The external power, the UPS, and the engine generators went inot a deadly embrace. The whole thing came down and would not come back up.

I take two lessons from this. First, redundancy adds some complexity and a lot of redundancy adds a lot of complexity. At some point the redundancy begins to introduce failure modes and failure events that would not have exited in its absence. There is an upper bound to such redundancy.

Second, test redundant systems through to resumption of normal operations.

In this case, the operators had tested to ensure that the redundant systems would come online in the event of a failure of the primary system. They had not tested to see what would happen when the primary system was restored to normal operation.

Who would have even thought about it? I confess that I would not have.

William Hugh Murray, New Canaan, Connecticut

✶ Re: Computers miss \$1.2M in ATM withdrawals (Fenner, [RISKS-18.53](#))

William Hugh Murray <0003158580@mcimail.com>

Fri, 18 Oct 96 11:03 EST

Some older readers of RISKS may recall the Franklin National Bank. An officer, speculating in foreign currency, lost fifty million dollars, a small percentage of the bank's capital. While the bank was able to keep this speculation secret for ninety days, it inevitably leaked and the leak resulted in an article in the Wall Street Journal. In the next ninety days the bank lost a billion and a half dollars in deposits and ultimately failed.

The lesson that most bankers take from the story is that publicity about losses is often worse than the losses themselves. In the electronic era, bank runs do not involve panic stricken crowds in the streets.

William Hugh Murray, New Canaan, Connecticut

✉ **Re: Health Info Database Misused (Fickeisen, [RISKS-18.53](#))**

William Hugh Murray <0003158580@mcimail.com>

Fri, 18 Oct 96 11:03 EST

> a public health worker took a laptop and disks with
confidential lists

This story would be very troubling if true. Just as troubling is the failure to provide a complete citation. In the absence of such citations, this story is merely hearsay, another modern myth.

I am reminded of the rumors, for example, of viruses, that are more destructive than the thing that they report. Another example is

the report
that Lexis/Nexis would return social security number for name.

In the electronic era, when gossip and rumors spread with
unprecedented
speed, it essential to know the primary source and to err on the
side of not
repeating that which you do not know first-hand to be both true
and
important.

William Hugh Murray, New Canaan, Connecticut

✶ People Security versus Computer Security

Li Gong <li.gong@Eng.Sun.COM>

Fri, 18 Oct 1996 21:52:29 -0700

Once again we are reminded that computer security should be
considered
within a wider context that includes people security. The
*Manchester
Guardian Weekly* (vol.155, no.14, for week ending Oct.6, 1996)
in its
Washington Post section (p.16) reported that a spy named Robert
Chaegon Kim
in the Washington D.C. area had been able to gather sensitive
information
and pass it on to a South Korean embassy official. The report
said that

"... Kim was an ideal source ... His computer work in what is
known as a SCIF (Secure Compartmented Information Facility)
behind
two secure doors at the Office of Naval Intelligence
afforded him
extraordinary access to a wide range of classified studies
and
analysis by many intelligence agencies."

The report went on to say that "Kim routinely removed the classified labels" before sending out the files. One might reasonably argue that the computer system was a significant help for Kim to do his "job". Bob Morris often says that "there will always be a Walker", and he is proven correct so far!

Li Gong, JavaSoft, gong@eng.sun.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 18: Issue 55

Weds 30 October 1996

Contents

- [S-Bahn stopped by new switching software](#)
[Debora Weber-Wulff](#)
- [Privacy: Bring back ticker-tape for the next N.Y. parade](#)
[Bruce R Koball](#)
- [Child Pornography Hoax](#)
[Edupage](#)
- [Risks of taking porno spam at face value](#)
[Pete Mellor](#)
- [Beating the GRE: What time zone are you in?](#)
[from Manny via Dave Farber](#)
- [Leonard Levine and Computer Privacy Digest](#)
[Peter G. Neumann](#)
- [A new use of a new crypto attack](#)
[Jean-Jacques Quisquater](#)
- [Re: A new attack on DES](#)
[Tony Lauck](#)
[Walt Farrell](#)
- [Characterization of Research](#)
[William Hugh Murray](#)
- [Re: \\$850 Million Social Security Problem](#)

[Mark Brader](#)

● [Re: Franklin National Bank](#)

[R Ken Brown](#)

● [Re: When is -32768 != -32767-1 ?](#)

[Mark Brader](#)

● [Wasted redundancy](#)

[Ian Brogden](#)

● [Info on RISKS \(comp.risks\)](#)

⚡ **S-Bahn stopped by new switching software**

Debora Weber-Wulff <weberwu@tfh-berlin.de>

27 Oct 1996 15:07:50 GMT

The Berliner Tagespiegel reported this week on the new light-rail switching software that was installed the same weekend that the light rail (S-Bahn) was moved back from the regular train track to its own tracks, which had been under repair for some time. The tracks were cut off all day Saturday and Sunday with busses attempting to move passengers. The software is installed at a central switching board, so that the transportation company can save the money they would otherwise pay real people to manually move the switches. The software kicked in, and Monday all went well until rush hour hit - yep, you guessed it, a stack overflow, just like in Hamburg. And it is the same large German company that was responsible for the Hamburg fiasco that wrote this software - it may even be the exact same software. Will they ever learn to *do* quality assurance at this company and not just talk about it? It took hours to get the system back up. The newspaper quotes

(ironically?) a spokesman as saying that the software control was very modern since there is only one point at which it can go wrong. Of course, if that single point goes wrong... I spoke this morning with a nameless higher-up at the transportation company, who just said "Software always has errors. We're just happy that no one gets killed when the software fails." He wouldn't believe me, when I said that we have ways of ensuring that software won't fail.

Debora Weber-Wulff Technische Fachhochschule Berlin,
Luxemburger Str. 10,
13353 Berlin Germany weberwu@tfh-berlin.de <<http://www.tfh-berlin.de/~weberwu/>>

🔥 Privacy: Bring back ticker-tape for the next N.Y. parade

Bruce R Koball <bkoball@well.com>
Wed, 30 Oct 1996 08:07:49 -0800 (PST)

As most of the known universe is aware (or soon will be, c being a constant), the New York Yankees won the World Series this year... so, yesterday, the Big Apple honored them with its traditional tribute, a ticker-tape parade... a modern twist to the event, however, is noted in the following excerpt from **The New York Times**, 30 Oct 1996.

> Ticker tape being an obsolete relic, people hurled everything from
> shredded paper to confetti to toilet tissue. In fact, several
> government agencies across from city hall dumped entire boxes of public

> and confidential records out the window, without troubling to
shred
> them. Down came checks issued by the New York City Housing
Authority
> and records of unemployment checks from the New York State
Department
> of Social Services.

...which goes to show that the risks to the privacy and
confidentiality
of public record systems are not engendered solely by computers
and
telecommunications technologies... ultimately they begin with
people...

[This should be no surprise to long-time RISKS readers. In
[RISKS-3.90](#),

30 Oct 1986, ten years ago to the day, I noted essentially the
same

scenario after the New York Mets won the 1986 World Series.
PGN]

⚡ Child Pornography Hoax (Edupage, 24 Oct 1996)

Edupage Editors <educom@elanor.oit.unc.edu>

Thu, 24 Oct 1996 14:04:07 -0400 (EDT)

The FBI is saying that the recent widely distributed e-mail
message inviting
recipients to buy child pornography is a hoax; the message was
apparently
sent from New York City. (*Ottawa Citizen*, 23 Oct 1996, A4)

⚡ Risks of taking porno spam at face value

Pete Mellor <pm@csr.city.ac.uk>

Tue, 22 Oct 96 11:32:07 BST

The following is the text of a letter which I faxed to The Editor, London Evening Standard, today:-

As the recipient of two different versions of the e-mail message supposedly advertising child pornography, I (like many others) at first assumed it was genuine and complained to our e-mail postmasters.

Although they take this sort of misuse of the Internet very seriously and are investigating it, they pointed out that the message is extremely unlikely to be genuine, particularly since it contained the name and home address of an individual. This opinion is shared by UKERNA, the authority responsible for the academic network in this country.

It is probably a ``spam'' or hoax in which a message is sent by a malicious person in such a way that it appears to come from someone else. The motive was probably to discredit or to cause other damage to the individual named in the e-mail message, damage which the article in your edition of 21 October has aggravated, since it actually names this person. A little elementary fact-checking would have been advisable.

(I was also amused to see that the messages I received came from electronic addresses on the America On-Line (AOL) service provider. AOL achieved fame a short while ago by allegedly refusing a subscription from a user on the grounds that four of the letters in the name of his home town constitute a rude word! [[RISKS-18.07](#) and 08])

Peter Mellor, Centre for Software Reliability, City University,
Northampton
Square, London EC1V 0HB, UK. Tel: +44 (171) 477-8422, Fax: +44
(171) 477-8585

✈ Beating the GRE: What time zone are you in? (from Manny)

Dave Farber <farber@cis.upenn.edu>
Mon, 28 Oct 1996 18:40:50 -0500

This scheme is pretty clever! Of course, it doesn't address the East Coast market, but one can take the tests in Europe too. I took the computer science GRE in Switzerland (got a perfect score too :-). That's a six hour time difference! It never occurred to me to make notches in my pencil to record the answers ...

I'm not sure what the charges are for prosecuting such a thing. Kobayashi's test-takers' answers are not copyrighted by ETS: the test takers are not given the answers together with a copyright notice.

Manny

College Test Cheaters Arrested

Federal prosecutors in New York say a California man has been arrested on charges of operating an elaborate scheme to help prospective graduate school students cheat on admission exams. Prosecutors say George Kobayashi ran a company that provided test-takers with correct answers in code on pencils that the students carried into the exam with them. Authorities

say Kobayashi
paid a team of experts to take each exam in New York City using
assumed
names. These experts then telephoned the correct answers to
Kobayashi's
office in Los Angeles, where the answers were quickly coded onto
pencils by
Kobayashi's employees and then provided to the cheating
students. The scheme
worked because of a three-hour time difference between the
cities.

✶ Leonard Levine and Computer Privacy Digest

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

Tue, 29 Oct 96 11:37:26 PST

For those of you who are recipients of the Computer Privacy
Digest
(comp.society.privacy) and are wondering why you have not
received any
issues lately, the moderator, Leonard P. Levine, just called me
to tell me
that he had a heart attack on 13 Oct 1996, followed by a
successful bypass
operation. He is recovering nicely and wants you to know that
the Digest
will eventually continue. He insisted that he would like to be
left alone
(please, no e-mail or telephone calls or faxes to him or to the
Digest until
further notice), although he said he would not be averse to
postcards
(Leonard Levine, Dept of EECS, University of Wisconsin-
Milwaukee, Box 784,
Milwaukee WI 53201) if postmarked no later than 13 Nov 1996 (to
stave off
readers of the RISKS archives many moons from now).

There are two interesting RISKS connections. While on the gurney being wheeled into the operating room, Leonard observed that on his chest was a piece of equipment from Marquette Electronics that had been designed by his students. (I presume he took great personal pleasure in the fact that it worked correctly.) He also says he learned a lot more about the medical privacy issues.

✦ A new use of a new crypto attack (Re: Shamir, [RISKS-18.54](#))

Jean-Jacques Quisquater <Quisquater@dice.ucl.ac.be>
Thu, 24 Oct 1996 00:08:55 +0200 (MET DST)

Research announcement:

Short cut for exhaustive key search using fault analysis:
Applications to DES, MAC, keyed hash function, identification protocols, ...

Jean-Jacques Quisquater,
UCL Crypto Group, Louvain-la-Neuve, Belgium, jjq@dice.ucl.ac.be

23 Oct 1996

(ABSTRACT and DRAFT)

I confirm that the timing attack was well known to designers of smart cards for some time.

--- Jean-Jacques Quisquater, Dec. 20, 1995, sci.crypt

I'm a bit puzzled by the excitement over error analysis attacks --

they've been known for some time to cryptosystem implementors ...
--- Paul Kocher, Oct. 20, 1996, comp.security.misc

How to find a secret key faster than the exhaustive search without the help of the differential analysis.

--- This paper

During the last months very interesting programs, papers and announcements were released about the (cryptanalytic) use of transient faults in tamper resistant (or proof) devices by:

- some well-known anonymous authors (in the payTV context; SFS);
- Anderson and Kuhn (applications well fitted to the real world); [See Ross Anderson's comments in [RISKS-18.52](#). PGN]
- Boneh, Demillo and Lipton: they specifically attack public key cryptosystems; their core attack bells an alert to the scientific community to publish faster;
- Biham and Shamir: they described how to obtain a secret key (e.g. for DES) using few ciphertexts.

This list is open, and we reserve some room in this paper for the - future unknown authors.

Here we describe a new use of such attacks in order to accelerate exhaustive keysearches in several contexts. We don't discuss if these attacks are feasible: our main goal is to enumerate all possible attacks and their cryptanalytic use against specific models. Knowing that will improve our trust about the current or future devices in order to obtain a reasonable level of security in a complete system.

Introduction

We suppose that the opponent is in possession of the secure

device, able to know the (external) inputs and the outputs and to apply some physical constraints in order to trigger some transient errors at some random locations (RAM, registers, ...). We suppose that these errors do not interfere with the program used by the computations: these errors only modify some data at some stage of the computation. We do not here discuss the possibility of permanent errors: it will be explained in the full paper (incremental permanent errors with possible use of several secure devices, ...).

They are many protocols where the input message and the corresponding output message are accessible to everybody including the opponent if the device is physically in the hand of the user (maybe for some short period of time):

Let f be a public cryptographic function, computed by some secure device

(smart card, secure black box, security hardware, ...),

k a secret key, stored by the secure device,

guessing its value is the goal of the opponent in this

paper,

n the number of bits of the key k ,

K is the set of all keys for f ,

N the number of possible keys in K ,

m an input message,

c an output message.

General protocol:

input: m

output: $c = f(m, k)$

Examples:

- encryption of m by any secret key algorithm (DES, IDEA, ...),
- decryption of m by any secret key algorithm (DES, IDEA, ...),

- computation of the hashing of m by the keyed hash function f (MAC, ...),
- m is a random number used by some identification protocol,
-

Such protocols need very often some protections against possible abuses from (well-chosen by the opponent) messages m (see Biham-Shamir, Matsui, Vaudenay, ...) or not so random numbers. One necessary condition is to avoid the discovery of k by exhaustive key search: such a general search algorithm is now described.

Key search algorithm:

Given m, c

Enumerate all candidate keys i from K

 Compute $f(m, i) = c_i$

 If $c_i = c$ then (output i and stop)

End of loop.

Mean work factor: $N / 2$.

Indeed, if we suppose that the key is unique for each pair (m, c) (it is not true for DES: they are sometimes collisions) then the number of computations of f is $N/2$ for the mean case and N for the worst case. The goal of this paper is to show how to improve such a complexity by the use of (randomly activated) transient faults in the secure device.

Model 1: Single fault in the secret key

- Working hypothesis:

the opponent is able to modify at a random location one bit of the

key k (the new transient key is then k^*) and to get the correct result of

$f(m, k^*)$; after the reset of the secure device by the opponent, the

internal secret key is again the correct one k . We suppose that the

random modification is equidistributed on all n bits of the key k .

- Key search algorithm: given m ,

1. Physical attack of the secure device:

Obtain the n possible pairs (m, c_j) where c_j is equal to $f(m, k_j)$;

k_j is the modified key k with the j th bit being flipped;

We need about $n \cdot \log n$ "questions" to obtain the n different pairs (by the coupon collector paradox: in some way the dual of

the birthday paradox), that is, if f is the DES for instance, about

300 accesses to the secure device.

2. Enumerative key search on an external key search machine:

Given m , the c_j 's

Enumerate (pseudo-) randomly all candidate keys i from K

Compute $f(m, i) = c_i$

If $c_i =$ one of c_j 's then (output $i^*=i$ and stop)

End of loop.

3. Key correcting algorithm on an external computer:

Given m, i^*, c ,

Enumerate the n values i coming from i^* with one flipped bit at

every n possible positions

Compute $f(m, i) = c_i$

if $c_i = c$ then (output i and stop) !the secret key is found!

End of loop.

Mean work factor: $(N / (2^n)) + n$.

Indeed, the first step is very fast, the second step needs the mean work

factor of the exhaustive key search divided by the number of bits of the key

(if we suppose that the modified keys are randomly distributed in the key

set K) and the last step needs indeed n computations of f .

For DES it means about 2^{49} computations: let us recall that one FPGA device in one proposed implementation (see van Oorschot and Wiener) is able to do about 2^{26} computations of DES, with key change, each second (using a pipelined implementation it is possible to compute a DES at each clock tick and we here suppose a very possible clock of 65 MHz). It means that one secret key will be recovered by such a small, accessible and inexpensive machine in 2^{23} seconds, that is, less than 4 months. With p FPGAs working in parallel that time will be divided by p . The comparison operation in step 2 needs a modification of such a machine (a very easy step in software): it is a simple modification and thanks to the paper [Desmedt, Quisquater, EUROCRYPT '87] it is possible to implement it in the case of many c_j 's without any large expense and using a very simple hash (non cryptographic) function.

Model 2: Multiple faults in the secret key

- Working hypothesis:

The opponent is able to modify at random locations one or several bits of

the key k (the new transient key is k^*) and to get the correct result of

$f(m, k^*)$; after the reset of the secure device, the internal secret key

is again k . We suppose that the random modifications are equidistributed

on all n bits of the key k . The main idea is that the opponent is able

with a high probability to change randomly few bits of the secret key.

It is easy to adapt the key search algorithm in that context. The complexity of the attack is directly related to the number of modified keys. The step 3 is also easy: if the key change is too large in relation to the number of flipped bits, it is sometimes necessary to skip the search and to begin a new one.

Model 3: Attacking several secret keys in parallel using several secure devices

It is easy to see that the first secret key will be found by a number of computations equal to the number needed for the two first models divided by the number of secure devices used in parallel. It means a very fast discovery in case of a massive attack.

In the complete paper we will explain

- how to filter efficiently the noise (transient errors with useless output),
- how to combine such an attack with the one by Biham and Shamir,
- how to resist to these attacks without expensive computations by the secure device,
- how this attack is useful to know for public key cryptosystems.

Conclusion

We describe a new use of the attack by transient fault in a secure device: without any new protection and if this attack is feasible it means that a secret key will be obtained by about $N / \log(N)$ computations

2

(or less!) instead of $N/2$ computations by the normal exhaustive keysearch.

In that case this attack is really shortening your keys.

⚡ Re: A new attack on DES ([RISKS-18.54](#))

Tony Lauck <tlauck@CERF.NET>

Mon, 21 Oct 1996 18:53:33 -0400

In the early days of DES, the US government called out another standard for use in conjunction with DES, Federal Standard 1027. As I recall, this standard called for redundant hardware or other means of ensuring that hardware malfunctions could not affect accuracy of encryption or decryption.

FED-STD 1027 was superseded by FIPS 140. The FIPS are available at <http://www.nist.gov/itl/lab/fips/>, where the version is FIPS 140-1, "Security Requirements for Cryptographic Modules".

I quote:

"Level 4 also protects a module against a compromise of its security due to environmental conditions or fluctuations outside of the module's normal operating ranges for voltage and temperature. Intentional excursions beyond the normal operating ranges could be used to thwart a module's defense during an attack. A module is required to either include special environmental protection features designed to detect fluctuations and zeroize critical security parameters, or to undergo rigorous environmental failure testing that provides a reasonable assurance that the module will not be affected by fluctuations outside of the normal operating range in a manner that can compromise the security of the module."

It seems reasonable that NSA knew of Differential Fault Analysis in the 1970's.

Tony Lauck tlauck@cerfnet.com

✦ Re: A new attack on DES (Shamir, [RISKS-18.54](#))

"Walt Farrell" <wfarrell@VNET.IBM.COM>

Tue, 22 Oct 96 09:34:35 EDT

I found this report interesting, but I think that it should have referred to

"random" rather than "unknown" cleartext messages.

Since the attack requires that the attacker have physical possession of the encryption device and the cleartext messages (in order to encrypt them multiple times) clearly the attacker has the capability of "knowing" the cleartext contents directly.

To work with truly "unknown" cleartexts, I would consider only attacks that dealt with just the cyphertext and didn't require access to the cleartext.

Walt

✦ Characterization of Research (Re: Shamir, [RISKS-18.54](#))

William Hugh Murray <0003158580@mcimail.com>

Wed, 23 Oct 96 07:14 EST

Last night I visited the National Cryptologic Museum. I got to click the wheels on an Enigma and was reminded of the story that the British had bugged a room in France and got information about the key from listening to the clicks when the key was entered.

Bruce Schneier reminds me that there are more ways to stress a crypto engine

than are dreamed of in my philosophy and that any phenomenon that can be observed from outside the engine that vary with its operation can leak information about the key. Jerry Leichter (*) reminds me that hiding these things is a constant battle and that is certainly confirmed by my experience. [* Spelling FIXED in Archive copy.]

The cryptographers can help by properly characterizing their work. As I understand the work reported by Biham and Shamir, it demonstrates that the recent work reported by Bellcore and and which they admitted that they had only demonstrated against implementations that implement algebraic algorithms can be extended and applied to Feistel algorithms. In both cases, what is reported is theoretical, at least in the sense that they have not yet been demonstrated against any existing engines. (Based upon the "sky is falling" calls that I have received from reporters, I can guarantee you that little of this is understood.)

While the theoretical target of their attack was the DES, this work tells us nothing new about the DES. One point of the report was that the DES was simply a chosen example of a broader class of algorithms that would yield to such an attack. It is not even aimed at the DES but rather at hardware implementations. Terry Ritter has suggested that it might be far less effective against software implementations. To characterize this work as "a new attack on DES" is inaccurate at best and seriously misleading at worst.

William Hugh Murray, CISSP, New Canaan, Connecticut

✉ Re: \$850 Million Social Security Problem (Lucero, [Risks-18.51](#))

<msb@sq.com>

Sat, 26 Oct 96 02:24:30 EDT

Scott Lucero writes:

> In the Daily Brief, the *Los Angeles Times* reported that, according to
> Social Security Administration officials, some 695,000 Social Security
> recipients have been underpaid since 1972, due to a computer program error.

Never having lived in the US, I have no familiarity with the detailed workings of Social Security. However, the fact that an error like this apparently went unnoticed for 22 years strongly suggests that either (1) nobody who was receiving these payments ever reported the underpayment, because none of them had any information about how the correct amount to be paid was calculated, or (2) the underpayments were reported by, and corrected for, a few cautious and diligent individuals, but nobody in the SSA ever looked for a programmatic reason why they had occurred. Either way the risks are obvious.

How DID the error finally come to light, anyway?

Mark Brader msb@sq.com SoftQuad Inc., Toronto



<>

Mon, 28 Oct 1996 09:36:52 -0600

From: "Brown, R Ken" <brownrkl@texaco.com>
Subject: Re: Franklin National Bank (Murray, [RISKS-18.54](#))

Surely it was the attempted secrecy that caused the banks's customers to lose their trust? What are they trying to hide? A press release along the lines of:

"We regret to announce that the XXXXX of the YYYYY department has been suspended from duty pending the outcome of an internal inquiry into an unexplained loss loss of ZZZZZ dollars. On the positive side, the incident shows that the Bank's internal audit mechanisms are fundamentally sound and helped contain the loss to a figure that we can easily absorb. We have learned lessons which will enable us to further tighten up our procedures in future."

Might have headed the whole thing off at the pass.

I'm sure that the culture of secrecy that surrounds banks actually encourages their customers to distrust them.

⚡ Re: When is -32768 != -32767-1 ? (Giles, [RISKS-18.49](#))

Mark Brader <msb@sq.com>
Sat, 26 Oct 96 02:08:58 EDT

Since there was no further followup after Bear Giles' item in [RISKS-18.49](#),

let me set this matter straight. Compiler quality is not involved; integer type sizes are. The expression `-32768` or `(-32768)` is valid on any C implementation, and must have the value `-32,768`. However, its type is implementation-defined: it is either `int` or `long`. On some implementations, the type `int` contains 16-bit values, so `32,767` is the largest `int` value; in that case the type of the constant `32768` is `long`, so the expression `-32768` must also be `long`. On all other implementations, `ints` are wider than 16 bits and the type of `-32768` is `int`.

In everyday contexts like

```
short s = -32768;
```

this distinction is immaterial. Either a `long` or an `int` on the right-hand side of the `=` sign will be successfully converted to a `short` with the value `-32,768`, if the type `short` can represent that value; if it can't (the range can be just `-32,767` to `32,767`), then of course neither one will work correctly.

But there are a few specific situations where the type of `-32768` does matter. Bear described one of them in his original posting: where the compiler issues a warning for every `long-to-short` conversion and then proceeds to treat a large number of warnings as an error. And the context mentioned above, the file `<limits.h>`, is another special case, because the C standard requires the macro `SHRT_MIN` to produce an expression

whose type is
int, not long. Hence on *some* implementations, SHRT_MIN must
be defined as
(-32767-1) or some other such workaround, not (-32768); but on
other
implementations, where ints are wider than 16 bits, the
definition as
(-32768) is as correct as the other.

Since the file <limits.h> contains information specific to the
implementation,
it does not need to represent it in a portable manner. Hence
Gnu C is within
its rights to use (-32768) there, but, and here is the risk, it
does not
follow that a user can safely extract that expression from that
system file
and expect it to work anywhere.

Mark Brader msb@sq.com SoftQuad Inc., Toronto

Wasted redundancy

Ian Brogden <BrogdIP@louisville.stortek.com>

Thu, 24 Oct 1996 18:48:44 -0700

Some of the discussions on redundancy and backup systems reminds
me of an
automotive assembly plant where I once worked.

The plant engineers and management were always very insistent on
having
redundant computer systems, even though a failure wasn't
catastrophic for
90% of the cases. Typically there was 45 minutes to an hours
worth of job
instructions printed on paper.

As a system implementor, I always argued that we spent as much
time ensuring

there was adequate hardware redundancy as we did removing faults from the software. More attention to fault removal would have eliminated enough of the reasons the plant wanted redundancy to make the redundancy overkill.

When the primary system finally failed, it took at least as long to activate the backup as it would have to fix the primary, but because there WAS a backup, everyone worked on getting the backup up first. Of course, the key reason it took so long to get the backup going was that there was so much stuff running on it because no one wanted to "waste" that extra hardware.

A Japanese customer of the same system took a different approach, and didn't order a backup. They felt it was much more important that the primary get fixed immediately if it broke, and could tolerate the few hours of downtime.

Ian Brogden, Toronto i.brogden@ieee.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 18: Issue 56

Thursday 31 October 1996

Contents

- [The next stage of Differential Fault Analysis](#)
[Adi Shamir](#)
- [AOL Bans All Mail from 53 "Junk Mail" Domains](#)
[Edupage](#)
- ["Fall back, free parking; spring forward, pay more"](#)
[Bear Giles](#)
- [Cruise Missile software bugs](#)
[Kofi Crentsil](#)
- [Tote Board Crash at Breeder's Cup](#)
[Tony Harminc](#)
- [ATM problems in Canada](#)
[Richard Akerman](#)
- [Re: Beating the GRE: What time zone are you in?](#)
[Li Gong](#)
[Bear Giles](#)
- [More Personal Information Databases](#)
[Lauren Weinstein](#)
- [Where Wizards Stay up Late: Book Review](#)
[Tom Perrine](#)
- [Info on RISKS \(comp.risks\)](#)

✦ The next stage of on Differential Fault Analysis

Adi Shamir <shamir@wisdom.weizmann.ac.il>

Thu, 31 Oct 1996 21:27:44 -0800

The Next Stage of Differential Fault Analysis:
How to break completely unknown cryptosystems, 30 October 1996
(draft)

Eli Biham, Computer Science Dept., The Technion, Israel
Adi Shamir, Applied Math Dept., The Weizmann Institute, Israel

The idea of using computational faults to break cryptosystems was first applied by Boneh Demillo and Lipton to public key cryptosystems, and then extended by Biham and Shamir to most types of secret key cryptosystems. [See [RISKS-18.54](#).] In this new research announcement, we introduce a modified fault model that makes it possible to find the secret key stored in a tamperproof cryptographic device even when nothing is known about the structure and operation of the cryptosystem. A prime example of such a scenario is the Skipjack cryptosystem, which was developed by the NSA, has unknown design, and is embedded as a tamperproof chip inside the commercially available Fortezza PC cards. We have not tested this attack on Skipjack, but we believe that it is a realistic threat against some smart-card applications that were not specifically designed to counter it.

The main assumption behind the new fault model is that the cryptographic key is stored in an asymmetric type of memory, in which induced faults are much

more likely to change a 1 bit into a 0 than to change a 0 bit into a 1 (or the other way around). CMOS registers seem to be quite symmetric, but most types of nonvolatile memory exhibit some degree of asymmetry. For example, a 1 bit in an EEPROM cell is stored as a small charge on an electrically isolated gate. If the fault is induced by external radiation (e.g., ultraviolet light), then the charges are more likely to leak out of the gate than to be forced into the gate.

To make the analysis simpler, we assume that we can apply a low-level physical stress to the tamperproof device when it is disconnected from power, whose only possible effect is to occasionally flip one of the 1 bits in the key register to a 0. The plausibility of this assumption depends on numerous physical and technical considerations, which are beyond the scope of this note.

We further assume that we are allowed to apply two types of cryptographic functions to the given tamperproof device: We can supply a cleartext m and use the current key k stored in the nonvolatile memory of the device to get a ciphertext c , or we can supply a new n -bit key k' that replaces k in the nonvolatile memory.

The cryptanalytic attack has two stages:

1. In the first stage of the attack, we keep the original unknown secret key k stored in the tamperproof device, and use it to repeatedly encrypt a fixed cleartext m_0 . After each encryption, we disconnect the device

from power and apply a gentle physical stress. The resultant stream of ciphertexts is likely to consist of several copies of c_0 , followed by several copies of a different c_1 , followed by several copies of yet another c_2 , until the sequence stabilizes on c_f . Since each change is likely to be the result of one more key bit flipping from 1 to 0 (thus changing the current key k_i into a new variant k_{i+1}), and since there are about $n/2$ 1 bits in the original unknown key k , we expect f to be about $n/2$, and c_f to be the result of encrypting m_0 under the all-zero key k_f .

2. In the second stage of the attack, we work our way backwards from the known all-zero key k_f to the unknown original key k_0 . Assuming that we already know some intermediate key k_{i+1} , we assume that k_i differs from k_{i+1} in a single bit position. If we knew the cryptographic algorithm involved, we could easily try all the possible single bit changes in a simple software simulation on a personal computer, and find the (almost certainly unique) change that would give rise to the observed ciphertext c_i . However, we don't need either a simulator or knowledge of the cryptographic algorithm, since we are given the real thing in the form of a tamperproof device into which we can load any key we wish, to test out whether it produces the desired ciphertext c_i . We can thus proceed deterministically from the known k_f to the desired k_0 in $O(n)$ stages, trying $O(n)$ keys at each stage. The attack is guaranteed to succeed if the

fault model is satisfied, and its total complexity is at most $O(n^2)$ encryptions.

This seems to be the first cryptanalytic attack that makes it possible to find the secret key of a completely unknown cryptosystem in polynomial time (quadratic time in our case). It relies on a particular fault model that seems to be realistic, but requires further study. In the full version of this paper, we'll discuss numerous extensions of the attack -- including the analysis of more complicated fault models in which the sequence of corrupted keys forms a biased random walk in the space of 2^n possible keys.

✶ AOL Bans All Mail from 53 "Junk Mail" Domains (Edupage, 29 Oct 1996)

Edupage Editors <educom@elanor.oit.unc.edu>
Tue, 29 Oct 1996 21:17:27 -0500 (EST)

America Online's new "Preferred Mail" junk e-mail blocking tool was activated several days ago on all 6.5 million accounts; it blocks all e-mail from a list of (currently) 53 network domains that AOL has identified as junk e-mailers. Many of the domains have been used in the past by Stanford Wallace, who is suing AOL for blocking his messages. One blocked domain, managed by an Internet service provider called Cybercom, has been tentatively removed from AOL's prohibited list, after protesting that it had

been placed on the list not because of its own actions but because two of its 1500 clients sent adult-oriented junk e-mail, causing AOL immediately to block all mail to AOL subscribers from any Cybercom customer. (*Atlanta Journal-Constitution*, 29 Oct 1996, D4)

[Following up on this strategy, the next step would be for AOL to block all mail from AOL! PGN]

🔥 "Fall back, free parking; spring forward, pay more"

Bear Giles <bear@tigger.cs.colorado.edu>
Wed, 30 Oct 1996 18:27:57 -0700 (MST)

The University of Colorado at Boulder has replaced the mechanical parking meters in severals lot with a centralized computerized version that prints a receipt convenient when challenging parking tickes. (Or is that "convenient for them," since you need this receipt to successfully challenge parking tickets? :-) The two spots I use are in prominent locations -- one is across from Regents Hall, the other is adjacent to the Police building. I mention this because one would expect parking lot monitors to frequent these sites...

Yet is it any wonder that I was a scofflaw during my classes on Monday afternoon (on the first school day after the return to Mountain Standard Time), since this high-tech solution to a simple problem made it impossible to pay for my first hour of parking?

The flip side is worse -- if ticketed I could make a legal

defense that

"what isn't permitted can't be compelled." Unlucky visitors in the spring can't make such a claim and may be forced to pay for an additional hour of parking.

Bear Giles bear@indra.com

✈ Cruise Missile software bugs

<crensil.k@atomcon.gc.ca>

Thu, 31 Oct 1996 07:41:46 -0500

I don't remember seeing anything in RISKS on software bugs deflating the success rates of recent cruise missile strikes on Iraq. It all sounds very similar to the Ariane-5 software reuse fiasco. Below are the relevant excerpts from David A. Fulghum's "Hard Lessons in Iraq Lead to New Attack Plan" in the September 16 1996 issue of *Aviation Week & Space Technology* (pp. 24-25).

The article states: "Bomb damage assessment of the initial cruise missile strike indicates that three of the 10 targets attacked by 13 Air Force CALCMs (Conventional Air-Launched Cruise Missiles) emerged with "no detectable damage," according to a U.S. intelligence report. The Boeing built CALCMs, converted from Cold War-era nuclear weapons at a cost of \$165,000 each, were launched from two B-52H bombers over the Persian Gulf."

Apparently: "Part of the problem with the CALCMs were that they were fired at targets they were not designed to destroy, a product of hasty planning, according to a senior Pentagon official. Air Force success rates were further deflated because of missile computer programming quirks."

Further on: "Another CALCM target escaped damage because of a software targetting quirk left over from its nuclear role. If two CALCMs are aimed at the same target at the same time, one of the missiles will re-aim itself at the next highest priority target. In the initial raid, one CALCM missed the target while the other went on to the next site."

The risks of reusing software without proper testing for the new application are obvious.

Kofi Crentsil (crentsil.k@atomcon.gc.ca)

🔥 Tote Board Crash at Breeder's Cup

"Harminc, Tony" <tzha0@toraag.com>

Wed, 30 Oct 96 15:34:00 PST

The Breeder's Cup - an American horserace being run for the first time in Toronto last Saturday - suffered from various organizational difficulties, according to an article in the Toronto Globe & Mail on Monday Oct. 28, 1996. Among these was that the "tote board" - the display of current betting odds - crashed.

"Betting was never halted during the tote board disruption, but

[Ontario

Jockey Club president David] Willmot said it probably cost about [CA]\$400,000 in local betting handle because serious players will not make

large bets unless they can see exact odds. It was a \$35,000 bet in US

currency that crashed the system. The software designed to convert US money

to Canadian in the tote pools could not handle such a large amount."

Hmmm... \$35,000. Do you suppose a bet of oh, say \$32,767 might have worked?

Tony Harminc tzha0@toraag.com

⚡ ATM problems in Canada

Richard Akerman <akerman@appliedmicro.ns.ca>

Wed, 30 Oct 1996 21:20:52 -0400

Toronto-Dominion bank's automated teller machines crashed for most of the

weekend, affecting the bank's 2000 machines. The TD debit payment system

was also down. In Canada, 80% of the banking is done electronically, and

the 30 million residents have 43 million bank cards. In a separate item,

some Royal Bank customers had their accounts debited but received no cash.

[There were 1.023 billion ATM transactions in 1995 (about 35 transactions

per year for every person in Canada).] [Source: Halifax *Daily News* 29 Oct

1996, p. 19. Reported in Canada by Rob Ferguson, The Canadian Press (CP)

agency, in many papers. PGN Abstracting.]

Richard Akerman rakerman@chebucto.ns.ca <http://www.chebucto.ns.ca/~rakerman/>

✉ Re: Beating the GRE: What time zone are you in? ([RISKS-18.55](#))

Li Gong <li.gong@Eng.Sun.COM>
Wed, 30 Oct 1996 13:43:23 -0800

The test-beating scenario could actually happen within the same time zone.

To gain entrance to a British graduate school, one usually is required to take ELTS, which is a British administered English language test that it similar to the American TOEFL. ELTS contains 6 exam subjects, including the normal listening comprehension as well as writing exams where one is asked to compose a long essay and a short one, in the space of one hour, for two given themes. I singled out these two exam subjects because they tend to be the more difficult ones for native Chinese speakers. (Oral exam by interview is probably more difficult, but it is almost impossible to cheat, except perhaps by hitting on a discussion topic that is favoured by the interviewer.)

About 10 years ago, the local British council was responsible for administering the tests, and they had four test sites: Beijing, Shanghai, Chengdu, and Guangzhou. They were (and are) in the same time zone but are hundreds of miles apart. The British council made things worse (1) by using a travelling team to conduct the tests, which meant 3 to 5 days delay

between two consecutive tests, and (2) by having only two sets of exam papers. The upshot was that snail mail could still allow a few days for one to fully prepare for the composition tests. It was said that a year earlier, an examiner noticed, during listening comprehension, that some students finished 100% correct papers when the tape was played only half-way through.

Li Gong, JavaSoft

✶ Re: Beating the GRE: What time zone are you in? (Manny, [RISKS-18.55](#))

Bear Giles <bear@tigger.cs.colorado.edu>
Wed, 30 Oct 1996 18:37:54 -0700 (MST)

> I'm not sure what the charges are for prosecuting such a thing.

Perhaps "falsification of legal documents"? The government has an obvious interest if a student is admitted and gets federally backed financial aid on the basis of fraudulent documents. Even if the student doesn't get direct aid, most public schools still receive indirect subsidies.

Bear Giles bear@cs.colorado.edu

✶ More Personal Information Databases [From PRIVACY Forum Digest 5 19]

Lauren Weinstein; PRIVACY Forum Moderator <lauren@vortex.com>

Mon, 14 Oct 96 13:27 PDT

PRIVACY Forum Digest
05 : Issue 19

Monday, 14 October 1996

Volume

Moderated by Lauren Weinstein (lauren@vortex.com)

Vortex Technology, Woodland Hills, CA, U.S.A.

The PRIVACY Forum is supported in part by the

ACM (Association for Computing Machinery)

Committee on Computers and Public Policy,

"internetMCI" (a service of the Data Services Division
of MCI Telecommunications Corporation), and Cisco Systems,
Inc.

As you probably have seen over the last few weeks, the topic of personal information databases has rather suddenly become a "hot topic" in the mainstream media, propelled partially by the Lexis-Nexis "P-TRAK" controversy. The Federal Trade Commission is reportedly considering placing Social Security Numbers (SSN) and some other related data back into the "protected" status of the Fair Credit Reporting Act [FCRA] (that is, removing SSN from the "publicly available" credit header category). There are also reports that Congressional efforts that were on track to **weaken** the FCRA may have been halted or reversed by the resulting public outcry.

But it's worth emphasizing again that we need comprehensive study and legislation to begin broadly addressing the entire privacy area; it is simply not possible for these problems to be addressed one service at a time.

As I pointed out originally, "P-TRAK" does not represent the most onerous of available databases. Lexis-Nexis **did** block name to SSN

lookups (though not the reverse), and has provided mechanisms to allow people to request removal (which may or may not be effective in the long run--time will tell). But they are at least trying.

There are other services that promote the availability of vast arrays of personal information that many people would (erroneously) consider private, with no removal options of any kind available. It's important to note that with all the services with which I'm familiar, there is nothing illegal or otherwise illicit about their operations. They're distributing "public record" and other openly accessible data not currently covered by the FCRA or other laws. Much of the data comes from public municipal databases, or from "business transaction" information of the sorts we've discussed previously, and over which little or no legislative restrictions exist.

It's also the case that there are legitimate reasons why some individuals and other entities might at times need access to some of the information contained in various categories of these databases. There are cases where some frauds can be prevented or traced through such information. The problem is that at present there are no legal requirements placing any sort of "need to know" on most of this data, so most is accessible essentially to anyone willing to pay the designated fee, regardless of their (good or bad) motives.

Many services are providing these sorts of data, some very large

and
some small. Outside of Lexis-Nexis "P-TRAK" with which we're
already
familiar, here's information regarding two representative
others...

-- "Information America" (<http://www.infoam.com>)

IA has a nicely laid out web site listing a veritable cornucopia
of public
record and other related available data. I won't even attempt
to give a
comprehensive listing here, but just a few of the many
categories include:

Wizard -- master search of all Information America online
services

Asset Locator -- real property, stocks, personal property,
etc.

People Finder -- Address Alert, Credit Bureau Headers,
Deceased Records, Neighbor Listings,
Person Locator, Skip Tracer,
Social Security Number Tracker, Telephone Tracker,
Trace a person's residential moves

Relationship Identifier, and so on...

This is but a small sampling. In a conversation with their
Executive VP,
I learned that, in response to concerns raised by the "P-TRAK"
furor, they
have very recently voluntarily removed SSN data from the credit
header
output information. Their web site has been recently updated
and no longer
shows SSN as an available data output item.

This puts them in the same category as "P-TRAK" in this respect,
in that you
can still *search* for other information using SSN if you
already know the

number, but you can't get an SSN from other data via Information America.

I was told that some of their clients engaged in criminal investigation type work were not at all happy at having the ability to lookup SSNs removed from everybody's access, since they consider it to be an important investigative tool.

Information America does not provide a mechanism for persons wishing to be removed from any of their databases. First, they feel that the public record data they supply would be less useful for legitimate purposes if people could opt-out at will. Secondly, they say that since some of the databases are not under their direct control, they do not have the technical means to provide such mechanisms in any case.

--- CDB Infotek (<http://www.cdb.com>)

CDB provides a range of services and data very similar to that of Information America. However, they have chosen *not* to block access to Social Security Number data. According to the customer service representative I spoke to, you can still look up a person's credit header record based on name, address, or other data, and obtain their SSN through the service (provided the SSN is included in that person's database record of course, which would typically be the case). CDB also promotes the availability of all information over the Internet. No obvious provision for requesting removal from their databases is apparent.

- - -

There are other similar organizations as well. It's a difficult situation.

In the absence of legislation addressing these issues across the board,

services who take unilateral actions to restrict any class of data feel

that they're putting themselves at a competitive disadvantage compared

with those services who *don't* implement such restrictions.

We need to start working out sensible, logical, and balanced rules and laws

regarding information and privacy, that address the concerns of a wide

range of individuals and organizations. The longer we wait, and the

more we approach the area in a piecemeal fashion, the more intractable

the problems are likely to become.

--Lauren--

✦ Where Wizards Stay up Late: Book Review

Tom Perrine <tep@SDSC.EDU>

Tue, 29 Oct 1996 17:07:04 -0800 (PST)

Where Wizards Stay Up Late: The Origins of the Internet
by Katie Hafner and Matthew Lyon, Simon and Schuster, NY NY
1996

(ISBN 0-684-81201-0)

Reviewed by Tom Perrine <tep@sdsc.edu> [See also [RISKS-18.29](#)]

The Internet has erupted onto the scene of mainstream consciousness in just a few short years. Numerous attempts to "explain" all this technology has lead to a plethora of books purporting to educate "everyman"

about the innermost workings of this technology. Out of this morass of poorly-researched books (and entirely too few good ones) comes something more interesting: a technological history of the Internet's direct ancestor, the ARPA network.

Coming seemingly out of nowhere, vaulting from the relative obscurity of a handful of research facilities into homes and schools across the country and around the world, the Internet is obviously the most important technological tool since the personal computer (some would say since movable type).

But where did the Internet come from? Was it created from whole cloth? Was it created by a single company? Why isn't it run by "The Phone Company?" What was the ARPAnet? Just who did invent the Internet, and when, and why?

All of these questions (and many more) are answered by the eminently readable book Where Wizards Stay Up Late: The Origins of the Internet. This book could be dismissed as simply The Soul of a New Network, but that would be a mistake. This book is more readable, yet more technically complete and accurate than Kidder's The Soul of a New Machine.

Katie Hafner and Matthew Lyon have successfully explained the origins of the technology that millions now depend on and take for granted every day. They take the reader on a journey that begins in the early days of the Cold War with the launch of Sputnik, and ends with today's commercial on-line services, and ubiquitous electronic mail and World Wide Web

addresses.

If you doubt that "the Net" has become important to average consumers, consider these questions: Has anyone seen a recent television commercial or magazine advertisement without an "http" in it lately? Why did the Cable News Network (CNN) have as its lead stories the recent network outages of America Online and BBN Planet that left literally millions without Internet access for more than a day?

Along the way, we are treated to the dreams of visionaries and charlatans, academics and bureaucrats, scientists and engineers, who shared the hope of using technology to connect people to people.

The story is organized chronologically, yet always sets the technology in the context of the people and the culture of the times. The book focuses on the earliest period of the ARPAnet, the original computer network research project funded in the 1960s by the US Department of Defense. This period is the least known, and the information about this period the most important to preserve at this time, while the persons involved are still around to tell (and debate) their stories.

This book is a first-class piece of historical detective work, piecing together developments at laboratories across the country and around the world, all of which dovetailed to produce the world's first geographically-distributed computer network.

The first chapters are devoted to the origins of the Advanced Research

Projects Agency (ARPA) itself, set in the days following Sputnik, and America's technology "wake-up call". The early advocates of "computer communications" are introduced, including Bob Taylor, Joseph Licklider ("Lick"), and Larry Roberts.

This book attempts (and mostly succeeds) in tracing the engineering decisions that shaped the ARPAnet's technology (and culture). The early debates of circuit-switched vs. packet-switched designs, centralized (star) vs. distributed (mesh) are all examined and explained in accessible, yet not over-simplified terms.

The origins of Bolt Beranek and Newman (BBN), and the people who worked there are described in some fascinating detail. Who would imagine that a consulting company that was formed to perform acoustical engineering for new buildings would become the builders of a computer network? The trials and tribulations of the "IMP Guys" that led to the creation of the first network "router", the ARPANET Interface Message Processor (IMP), introduces two people who would continue to connect people and computers: Willie Crowther (original author of "ADVENTURE"), and Bob Kahn, who started the Strategic Computing Program, which is the more formal name for the "Information Superhighway" program of the U.S. government. The late nights, and the eradication of "the bug" on the eve of the first IMP's shipment from Cambridge to California are all recounted in a no-nonsense, technically-savvy style.

Later chapters describe the activities at SRI, the original Network Information Center (NIC), and the culture and people who decided that a network standards document should be a "Request For Comments" (RFC).

These RFCs, and a culture of openness have been blamed (or praised) for the demise of the International Standards Organization (ISO) Open System Inteconnect (OSI) network protocols; the closed, agonizingly slow process of ISO standardization process was continually "overcome be events" as the ARPANET folks pushed the envelope with "rough consensus and running code".

Along the way we meet the first RFC, by Steve Crocker, titled simply "Host Software", followed by the first higher level protocols, documented by Jon Postel, Vint Cerf, the "MsgGroup" and the network's first "flame war" (over e-mail standards), the now-infamous "header wars".

The ARPANET's direct contribution to Artificial Intelligence research, operating systems (including UNIX), and human communication are all explored as well.

It's an interesting journey, told through the eyes of the pioneers that blazed the trail. But make no mistake, this book is about the people behind the technology as much (or more) than about the technology itself. Having essentially "grown up" on the net (my first ARPANET host account was active in 1976, when I was in high school), I was fascinated by the stories of the people who made all this communication possible. This book has

filled in
all the background of the happenings that I was too naive (or
busy with
school :-) to understand at the time.

The authors of this book have reached back to the original
sources, they
have spoken to and interviewed many of those who were directly
responsible
for the work described. In many cases the authors have reached
into the
ARPA/IPTO Oral History project tapes and distilled this
collection of
interviews into a seamless, coherent picture.

This book is about the people who invented the technology and
culture of the
Internet, the legacy of practical engineering, and "rough
consensus and
running code."

Tom E. Perrine (tep@SDSC.EDU) | San Diego Supercomputer Center
<http://www.sdsc.edu/~tep/> | Voice: +1.619.534.5000



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 18: Issue 57

Tuesday 5 November 1996

Contents

- [Cutting off husband's cybersex leads to assault](#)
[Mich Kabay](#)
- ["Software explosion rattles car makers"](#)
[Daniel P. B. Smith](#)
- [No power ==> no-see windows](#)
[Mich Kabay](#)
- [Lawyers eager for millennium cases](#)
[stayton](#)
- [More risks in the supermarket; polymorphic buttons](#)
[Dan Ruderman](#)
- [ATM Fraud in Israel - The Polish Gang](#)
[Jonathan Rosenne](#)
- [IRS to send tax information to mortgage brokers by e-mail!](#)
[Erann Gat](#)
- [Tracking Smart Cash](#)
[Edupage](#)
- [Office 97, VBA 5.0, and macro viruses](#)
[Rob Slade](#)
- [Re: Aerooperu](#)
[Peter G. Neumann](#)

- [Re: Tote Board Crash at Breeder's Cup](#)
[Ben Morphett](#)
 - [Fault-induced crypto attacks and the RISKS of press releases](#)
[Paul C. Kocher](#)
 - [Re: A new attack on DES](#)
[Vadim Antonov](#)
 - [Unintentional Accesses](#)
[John R. LoVerso](#)
 - [Accidental Shootdown of the F-15, once again](#)
[Chiaki Ishikawa](#)
 - [-32768, hopefully for the last time](#)
[Kurt Fredriksson](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✂ Cutting off husband's cybersex leads to assault

Mich Kabay <75300.3232@CompuServe.COM>
01 Nov 96 16:04:02 EST

Here's yet another RISK, from erasing programs:

Marion Walton, an Arkansas man, was discovered having a cybersex affair with a Canadian woman. In response, his wife Pat apparently erased his mail program. In retaliation, he apparently beat her, twice. ``Police are suggesting she file charges.'' [Source: Man beats wife after she pulls plug on cybersex, Reuters World Report, datelined Little Rock, 31 Oct 1996, via CompuServe's Executive News Service, PGN Abstracting.]

[Perhaps her husband will have to use his credit card to charge files -- that is, the kind that can be used to file down the iron bars? PGN]

⚡ ``Software explosion rattles car makers''

"Daniel P. B. Smith" <dpbsmith@world.std.com>

Tue, 5 Nov 1996 09:29:45 -0500 (EST)

Automakers [are facing] runaway growth in the lines of code their engineers must write and manage as microprocessors take over automotive functions...
``Software is where the problem is today,' said William Powers, VP of research at Ford. ``Today, if you change a line of code, you're looking at the potential for some major problems. Hardware is very predictable, very repeatable. Software is in much more of a transient state.''
The volume of code is exploding as processors proliferate behind the dashboard and under the hood. The typical auto has 10 to 15 processors; high-end cars can have as many as 80 ... ``An engine controller can have 100,000 lines of code'' [according to a Bosch VP]. [``Software explosion rattles car makers'', *Electronic Engineering Times*, 28 Oct 1996, front page.]

Daniel P. B. Smith dpbsmith@world.std.com

[Auto-mation has certainly arrived. PGN]

⚡ No power ==> no-see windows

Mich Kabay <75300.3232@CompuServe.COM>

04 Nov 96 17:01:04 EST

Here's a tidbit from the ever-interesting INNOVATION 96.11.04 (editors John Gehl & Suzanne Douglas <gehl@newsscan.com>, <douglas@newsscan.com> [The folks who bring you Edupage]):

Electric Shade

Researchers at Vrije University in the Netherlands have developed a light-blocking window film that can be adjusted by turning a switch. The film uses yttrium hydride, a metallic compound, which can block the sun completely, partially, or can be made transparent by using a small battery to alter the voltage passing across the film. The higher the voltage, the more hydrogen atoms, which causes the film to change from a metal to a semiconductor. The result is a clear window. Scientists plan to use the new product in automobiles, sunglasses, houses and other applications.
(*Popular Science*, Nov 1996, p31)

Great, eh? One needs a voltage in order to have a clear window. Lose power in your automobile and you lose visibility through your window. Let's hope they build in appropriate fail-safes in automotive applications....

M. E. Kabay, Ph.D. / Director of Education, NCSA (Carlisle, PA)

[Now you can have an yttrium atrium. If solar powered, it could blacken out on dark days when you need the light most. The next step might be pay-per-view windows? PGN]

Lawyers eager for millennium cases

<stayton@ibm.net>

Mon, 04 Nov 96 20:37:33 -0500

Lawyers eager for millennium cases: The year 2000 glitch that may trip up computer calendars could bring a slew of lawsuits, by Christian Plumb, Bloomberg Business News, *News & Observer*, Raleigh, NC, Sunday, 3 Nov 1996, page 5F

"It's just a gold mine", "It's like a law-school case of tort issues".

Charles R. Merrill, of McCarter & English, Newark, NJ.

Perhaps IT managers will take better notice of the year 2000 problem --
if lawyers start getting on their case.

[The thought of lots of these little cases filled with surprises suggests tortellini, he said, saucily. PGN]

✶ More risks in the supermarket; polymorphic buttons

Dan Ruderman <dlr@quake.usc.edu>

Fri, 01 Nov 1996 15:46:48 -0800

I was shopping for our Halloween party the other day, picking out all sorts of pricey nibbles and alcohol for our guests. At our local Vons (one of So. Cal's biggest supermarket chains) checkout is generally fast and straightforward, and I do not out of habit bother to check my receipt. But this time the price just seemed too high (perhaps I should just un-refine my tastes?)...

A quick glance revealed an obvious suspect: the same entry for a bottle of wine, printed and charged twice. The apologizing checker handed

me the correct refund, and I asked how this could happen. Apparently the first time you swipe alcohol through for the customer you are supposed to press a button which confirms their legal age status. But from that point on the very same button means "buying two of those". In my case, the checker simply forgot that she had run a six pack through already by the time the wine came, and so she "confirmed my age" twice. I do not know how widespread this particular system is, but if it is in all Vons stores, then it's plenty wide enough to be a potential problem. She noted and corrected the mistake so quickly that I suspect this circumstance is anything but rare.

RISKS readers are well aware of the danger associated with giving a single control two widely different meanings. If any job leaves a worker especially prone to forgetfulness (just through the sheer repetitiveness of the work), it's being a grocery store clerk. Two lessons: 1) check those receipts, and 2) keep all your liquor purchases together; that way the checker is less likely to forget.

Dan Ruderman

⚡ ATM Fraud in Israel - The Polish Gang

Jonathan Rosenne <rosenne@NetVision.net.il>

Sat, 02 Nov 1996 17:05:24 +0200

Yediot Aharonot, October 23, 1996

A judge in Tel Aviv has ordered the remand in custody of two additional suspects in a major ATM fraud case, who will join five businessmen from Poland. The gang are suspected of having prepared thousands of counterfeit ATM cards. The police claim they had purchased tens of thousands blank plastic cards in Greece, on which they recorded the magnetic stripe and on each there was a sticker with the PIN. A Israeli computer expert, Daniel Cohen of Ramat Gan, also in custody, obtained the codes and manufactured the cards. The Polish businessmen financed the operation, and planned to bring foreign workers from Poland to use the cards to withdraw money from ATMs. The police have photographs of suspects standing next to ATMs holding quantities of forged cards. They had used them to withdraw 1,500 Israeli Sheqels (500 US Dollars) each, to a total of IS 600,000 (US \$200,000).

Jonathan Rosenne, JR Consulting, PO Box 33641, Tel Aviv, Israel
+972 50 246 522
+972 50 246 522 http://ourworld.compuserve.com/homepages/Jonathan_Rosenne/

✶ IRS to send tax information to mortgage brokers by e-mail!

Erann Gat <gat@aig.jpl.nasa.gov>
Sun, 3 Nov 1996 10:23:09 -0800 (PST)

A prototype e-mail program linking IRS tax databases with participating

mortgage lenders is scheduled to get underway in the next few months in

California, run by the Fresno IRS office. Under the prototype program,

lenders will e-mail authorizations by home-loan applicants to the IRS,

allowing the agency to quickly e-mail tax data -- typically the applicants'

adjusted gross income for one or more years -- back to the lender.

[*LA Times*, 3 Nov 1996, Business section first page]

The article goes on to say that this information will be used both to verify

the information on the loan application, and to trigger IRS audits in cases

where the income reported on loan applications is more than what was

reported on tax returns.

There is no mention in the article about what if any measures are being

taken to ensure that this sensitive data is protected and authenticated.

Given the ease and regularity with which e-mail is misdirected, intercepted,

and forged, and the power that the IRS has to completely screw up your life,

I'd say this is the scariest thing I've seen in a long time (and as recent

readers of RISKS can attest, that is saying something).

Erann Gat

gat@jpl.nasa.gov

gat@power.net

✶ Tracking Smart Cash (Edupage, 3 November 1996)

Edupage Editors <educom@elanor.oit.unc.edu>

Sun, 3 Nov 1996 15:41:37 -0500 (EST)

A senior Justice Department official has urged makers of smart

carts to include a mechanism for tracking transactions over a certain dollar amount. Assistant Attorney General Robert Litt also called for "sensible limits" on how much value can be stored or transferred on a single card or PC. The government hopes it can work with industry without stifling smart card development, and without compromising individual rights. "We don't want to dictate how these features are designed, but there are certain reasonable parameters that industry should build into their systems," says Litt. (BNA Daily Report for Executives 29 Oct 96 A24)

🔥 Office 97, VBA 5.0, and macro viruses

Rob Slade <roberts@mukluk.hq.decus.ca>
Thu, 31 Oct 1996 15:47:41 EST

Good news from those fun guys and gals at Microsoft! According to an article on page 19 of the October 1996, edition of Datamation, Office 97 will include VBA (Visual Basic for Applications) 5.0 as the scripting and integration language for Access, Excel, PowerPoint, and Word. Not only that, but Microsoft has followed up on its promise to license VBA to other vendors: upcoming releases of Visio (Visio), Chameleon (NetManage), Photoshop (Adobe), and even AutoCAD (Autodesk) will use VBA 5.0.

To date, with the possible (though unlikely) exception of the recent Excel macro virus, successful macro viruses in the wild have been

confined to
Visual Basic for Word. The report has no details regarding the
level of
"backward compatibility" of VBA 5.0 with VBW, so I don't know
yet whether
Concept and its ilk will continue to propagate on through Office
97 and
other VBA 5 compliant applications. Even if they require
patching, the new
VBA 5 viruses will have a much greater platform base, and
therefore faster
creation and wider spread.

Office 97 shipments will begin to selected customers in
December, with boxes
due on retail shelves in late January of 1997.

roberts@decus.ca rslade@vcn.bc.ca slade@freenet.
victoria.bc.ca
link to virus, book info at [http://www.freenet.victoria.bc.ca/
techrev/rms.html](http://www.freenet.victoria.bc.ca/techrev/rms.html)

✶ Re: Aeroperu crash (Ladkin, [RISKS-18.51](#))

"Peter G. Neumann" <neumann@csl.sri.com>
Tue, 5 Nov 96 8:31:05 PST

A possible cause of the Aeroperu crash is mentioned in the media
this
morning. Crash investigators are considering whether some of
the plane's
sensor ports ('`static ports'') might have been left with
protective duct
tape covering them when the plane took off. (*San Francisco
Chronicle*,
CNN, etc.) It is apparently normal maintenance procedure to
cover the ports
(marking them with bright "Remove Before Flight" markers), to
prevent them

from getting clogged. [Indeed, it might seem surprising that forgetting to remove the covers does not happen more often.]

✶ Re: Tote Board Crash at Breeder's Cup (Harminc, [RISKS-18.56](#))

Ben Morphett <ben@jna.com.au>

Tue, 5 Nov 1996 16:16:40 +1100 (EST)

> Hmm... \$35,000. Do you suppose a bet of oh, say \$32,767
might have
> worked?

I'm tired of dumb bugs like this tripping us up.

To my mind they are as silly as bugs which arise in programmes because of fixed length strings, such as the famous one in sendmail where it didn't check the size of a string it was strcpy'ing into a fixed length buffer.
(Internet worm bug - brought down 10% of the Internet.)

Fixed length integers have the same kind of problems. If they are limited to 2 bytes or 4 bytes at compilation time (either because the author "knows" that there will never be the need for them to be any bigger, and then the programme is used by someone else, or more usually, the author didn't think about it at all), then all someone needs to do is enter 5000000000 at the prompt, and it will behave much more stupidly than if you try a number in the range that the programme is expecting.

What I'd like is compiler support for integers, not a subset of them, in

much the same way that you get compiler support for strings, not just strings of a fixed length.

Presumably it would malloc some space, and might have to do arithmetic in more than one machine instruction, and yes, this would be much slower than having a fixed 4 bytes sitting there. But often I don't care if programmes are slow, just as long as they are correct.

Ben Morphett ben@jna.com.au (02) 9935 5746 International:
+612 9935 5746

⚡ Fault-induced crypto attacks and the RISKS of press releases

"Paul C. Kocher" <pck@best.com>

Fri, 1 Nov 1996 05:59:54 -0800

I've been watching the recent announcements about fault-induced cryptanalysis with interest [e.g., [RISKS-18.50](#),52,54,55,56].

Whereas the attacks are extremely powerful tools, they aren't at all new to the crypto community -- there has been widespread discussion for years about these, they've been implemented by criminals and security system evaluators, and they are reasonably well documented.

For example, NIST specifically discuss such attacks and the need to prevent

them. FIPS PUB 74-1 (see <http://csrc.nist.gov/fips>),

"Guidelines for

Implementing and Using the NBS Data Encryption Standard," was published way

back in 1981 and says in section 5.2.2 on Error Handling:

> Errors associated with the primary encryption device should be
> detected and handled by the secondary device. Physical tampering detectors
> (vibration or intrusion sensors) may be used to detect physical tampering
> or unauthorized access to the encryption unit. Sensors which detect
> abnormal changes in the electrical power or the temperature may be used to
> monitor physical environment changes which could cause a security problem.
> However, the major requirement for error detection or correction involves
> the application itself. The type of error control utilized will depend on
> the sensitivity of the data and the application. The method selected may
> range from no error handling capability for some systems to full redundancy
> of encryption devices in other systems. Errors may be ignored when detected
> or the entire system may be immediately shutdown. Errors which could
> compromise the plaintext or key should never be ignored.

Anyone interested in issues relating to secure hardware design should also
study FIPS 140-1, "Security Requirements for Cryptographic Modules." It's
the best public document I know of for anyone designing tamper resistant
hardware and does a great job of covering the basics and also describes
measures to prevent these attacks, suggests using "two independent
cryptographic algorithm implementations whose output are continually
compared in order to ensure the correct functioning of the cryptographic
algorithm," etc. In general, these attacks are fairly straightforward to
implement once the appropriate errors are available.

In addition to published sources, I've had many discussions with other cryptographers error attacks and other hardware issues. (Ross Anderson in particular is extremely knowledgeable about hardware attacks and has done much to raise awareness about them. [See [RISKS-18.52](#)]) It's also important to note that there are also quite a few other attacks which haven't been published but which are widely known to the community. (For example, I've discussed widely my work on using timing attack math to analyze power consumption, use of error analysis to reverse-engineer secret algorithms, implementations of attacks using software pointer errors to damage secret keys and encryption function tables, etc.)

With the timing attack I was alarmed by the amount of confusion and misinterpretation that followed my initial release of the paper (though I didn't send out any press releases or contact any reporters), even though it been reviewed by many cryptographers prior to its release and was available online. I haven't seen the actual Bellcore paper yet and don't know whether it was reviewed before they sent press releases to the media, but in general I worry about the consequences of the public trying to evaluate the importance, novelty, and quality of unreviewed work.

Paul Kocher pck@cryptography.com (or <http://www.cryptography.com>)

✦ Re: A new attack on DES (Lauck, [RISKS-18.54](#))

Vadim Antonov <avg@pluris.com>

Fri, 1 Nov 1996 15:07:24 -0800

I would venture to guess that a simple replication of the encryption circuitry, combined with a circuit that would suppress output if results are different would make the box fairly resistant against DFA.

That can be improved further if several substantially different implementations are used, so that identical environmental factors will not cause identical failures. The added benefit is better resistance against current-draw and timing attacks.

: It seems reasonable that NSA knew of Differential Fault Analysis in the
: 1970's.

The idea to break the "black box" to learn something about it is certainly not new. In fact, this is one of the most powerful tools in neuroscience and psychology (applying chemicals or current and watching the results, or investigating injuries to different parts of brain). However, there's a long way from the idea to the practical application.

--vadim

[A similar replication notion was also suggested by
Laurentiu Badea <bytemare@lmn.pub.ro>.]

✦ Unintentional Accesses (Re: Wanted Poster, Eckenwiler, [RISKS-18.51](#))

"John R. LoVerso" <j.loverso@opengroup.org>
Fri, 11 Oct 1996 15:10:47 -0400 (EDT)

In [RISKS-18.51](#), Mark Eckenwiler wrote:

> Of course, the FBI has had the Ten Most Wanted up in a web
page here
> in the US for some time; see [http://www.fbi.gov/mostwanted/
tenlist.htm](http://www.fbi.gov/mostwanted/tenlist.htm)

My favorite thing to do when handed such a URL is to strip off
the filename
and try to access the directory. The URL [http://www.fbi.gov/
mostwanted/](http://www.fbi.gov/mostwanted/)
brings up a conveniently hyper-linked listing of all the
contents of that
directory. This is usually not what the creator of those web
pages
intended. Sometimes there are additional documents or images
that you
wouldn't otherwise be able to find, because they are not
referenced from any
of the links in an advertised URL.

Using the terms "filename" and "directory" in the previous
paragraph is
old-style web talk. New-speak suggests the terms "trailing path
component"
and "containing object", respectively. This is to emphasize
that "web
space" doesn't necessarily map into files and directories, but
can be
ephemeral data.

Unfortunately, the use of abstract terminology combined with the
default
settings on web servers tend to confuse the neophyte "web
designer". Their
lack of understanding leads them to create collections of pages
in which
there are files that they *think* are hidden from view.

In the FBI example, everything in the directory listing was referenced from a link on original URL. Many times this is not the case. Another example comes from a company that hired an outside 'expert' to create a survey for people visiting their web site to fill out. The survey was made accessible at a URL ending in ".../survey/surveyform.htm". Trying a URL with just the ending directory component (".../survey/") brought up a surprise. Not only did it give a directory listing showing the files making up the survey, but also included the a file holding the results posted to the survey form! Very interesting reading, especially for their competitors!

Not all web servers will automatically convert directory accesses into fancy indices this way. Most have this as an option. Usually an index is created only when there is no manually created index file (commonly called "index.html"). In fact, had the files "topten.htm" or "surveyform.htm" in these examples been called "index.html", then not only would the URLs have been shorter, but a directory listing would have been made unobtainable.

Hence, the solution is a combination of: avoid letting neophytes create your web pages, fix your server, and know what you are doing before you release it to the world. Of course, there is far too much momentum on the WWW for any of these to come into play these days.

As a parting thought, I wonder if any of the common web search engines strip off trailing path components when indexing sites. Normally a spider will

work by collecting the graph of pages available by walking the "advertised" pages (which, in my own work, is called a "weblet"). By trying a path stripping approach, they might end up with a slightly "richer" index.

John R. LoVerso, Open Group Research Institute

✦ Accidental Shootdown of the F-15, once again

Chiaki Ishikawa <ishikawa@personal-media.co.jp>

Fri, 1 Nov 1996 21:41:12 +0900 (JST)

Earlier [[RISKS-18.18](#), 18.41], I reported on the accidental shootdown of a Japanese air force F-15 plane by a sidewinder missile from another plane during training and the subsequent handling of the case by the air force and the prosecutor's office.

Now, the Japanese Air Force has taken an unusual step of adding a new finding to its previous report citing that the 30 years pilot in question changed its testimony to "he may have possibly turned off the safety mechanism although he had no clear recollection of having done so" from the earlier "he had not touched the safety mechanism". (Translation mine.)

This additional finding to the accident investigation has been reported in at least one Japanese national newspaper(ASAHI) and a major news channel, NHK this morning. According to the NHK news the change of a finding issued

by an investigation committee has been very rare among defense community.

A little more detail. After the case was sent to the local prosecutor's office, the prosecutor's office decided that the pilot cleared the safety mechanism. (I have absolutely no idea how the office reached this conclusion.) However, his case has not been sent to the court. The prosecutor's office decided not to pursue the case there. (I don't know the English phrase for this, but the office seems to think the merit of doing so is considered less than the hassle/time/money of pursuing the case in the court and is not worth the crime(? I am not sure if this is the right word here.) committed.)

After the prosecutor's office concluded differently from its own investigation committee, the Japanese air force questioned the pilot again, and his testimony changed as noted above. Originally, the report mentioned possible unknown hardware (electric circuit and such) malfunction.

So the cause finally seems to me a human error of a sort. Pilot himself, and my main contention that whoever organized the training ought to have missiles removed in the first place, and maybe ordered a placement of a little gadget (even a paper cup will do as the previous discussion showed.) over the safety switch to avoid accidental touching. I wish the higher-ups are criticised more in the press, but not so far.

PS: I missed joining the discussion of publicly discussing the cause of (air) accident in an open forum, which took place after my

previous post re
prosecutor's office receiving the case of pilot. Problem was
that my
workstation was replaced and the printer hooked to it had to be
reconfigured. I usually print Risks digest on paper, and read it
on the
commuter train. Only recently, the printer became back online
and I printed
the backlog issues on paper and followed the thread. I can only
observe the
following myself now.

- Public scrutiny is not necessarily a bad thing during a formal
investigation continues provided that the
information accessible to the chosen "experts" is also made
available.

Beside the chosen experts, there are equally qualified people
elsewhere.

- Of course, the information may not be released to the public
due to
legal and other reasons. This makes it very difficult to
expect
"intelligent" discussion from the public, I agree.

- I noticed that the military wanted to make sure the career of
the
pilot is not unnecessarily destroyed. His name was only
revealed
after there was news that his case was now handled by the
local
prosecutor's office.

Today's Asahi newspaper, and NHK news in the morning
didn't mention the name. Maybe because the prosecutor's office
decided not to pursue the case in court?

- When I think about this, the public debate can ruin the
career of
possibly innocent people. If the shoot down of the F15 had
been
really due to flakey hardware, the pilot would have been
really

in an uncomfortable position to convince others that it was the fault of hardware produced by contractors with billion-dollar budgets.

The recent plight of a security guard who found the bomb in Atlanta during Olympics games comes to my mind.

So we must consider about this human element when we discuss these things in an open forum, too. Someone pointed this out to me and this point is well taken.

At the same time, not that I want to take side in this discussion, but please bear in mind that all the pieces I reported have already been reported in Japanese mass media such as national newspapers (each has circulation of a few million, I think) and national TV. (PGN kindly noted this.) So, by the time you read about the topic, at least a few million Japanese readers must have seen it already.

Anyway, just wanted to let you know what is going on in Japan.

Chiaki Ishikawa Personal Media Corp. Shinagawa, Tokyo, Japan
142
ishikawa@personal-media.co.jp

✉ -32768, hopefully for the last time (Re: Brader, [RISKS-18.55](#))

Kurt Fredriksson <etxkfrn@aom.ericsson.se>
Thu, 31 Oct 96 13:00:46 +0100

I read Mark Brader's contribution (18.55) and was a bit lost. I

can well

understand that badly designed compilers can cause problems, but what

puzzles me is that this discussion misses the fundamental background with

2's-complement representations: with 16 bits, -32768 is the smallest value

that can be represented, and 32767 is the largest value that can be

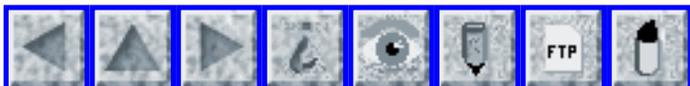
represented. What more is there to say?

Kurt Fredriksson, Moelndal

[Last time in RISKS? That would be a first time! The saga continues. 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 18: Issue 58

Weds 6 November 1996

Contents

- [1996 Melbourne Cup off-course betting fiasco](#)
[Harley Mackenzie](#)
- [Fidelity Brokerage computer problems](#)
[George C. Kaplan](#)
- [Bug in the network: a real spider](#)
[Nick Brown](#)
- [Announcement - Warning to Crypto and Banking Communities](#)
[Ross Anderson via Bruce Schneider and Monty Solomon](#)
- [Differential Fault Analysis: a possible defence?](#)
[David R Brooks](#)
- [Ping o'Death from Windows 95](#)
[Nick Brown](#)
- [Re: Office 97, VBA 5.0, and macro viruses](#)
[Otto Stolz](#)
- [Web search engines find connected components](#)
[David Skillicorn](#)
- [Re: Tote Board Crash at Breeder's Cup](#)
[Larry Kilgallen](#)
[Ian Rogers](#)
[Henry G. Baker](#)
- [Re: -32768](#)
[Paul Eggert](#)

[Dik Winter](#)

● [Info on RISKS \(comp.risks\)](#)

🔥 1996 Melbourne Cup off-course betting fiasco

<hjm@world.net>

Wed, 6 Nov 1996 14:10:15 +1100 (EST)

The Melbourne cup is Australia's premier horse race (handicap over 3200 metres with over \$AUS 2 million prize money), that even has its own public holiday in metropolitan Melbourne. The whole nation stops to listen or watch the race and lots of once a year punters have a dabble on the cup. The TAB (used to stand for Totaliser Agency Board when government owned and run, but now a public company) is the ONLY (legal) provider of off-course racing betting in Victoria.

However, when the punters turned up at their local TAB (or pub TAB located in hotels) to place their bets on yesterday's race (5 November 1996) there were queues that stretched out the door for hundreds of meters. The 15 year old computer system had failed again on Melbourne Cup day and most small agencies were off-line from about 10:45 am (AESST) to just before or after the running of the cup at 3:20pm (AESST), whilst the larger agencies were off and on with reduced numbers of active windows throughout this period.

Irate punters and TAB agency owners were, of course, furious and a lot of money that would have been wagered was lost as punters gave up waiting to try to get a bet placed. The TAB chief executive, Ross Wilson

(already controversial due to his seemingly excessive salary package) was quoted as saying that the system breakdown "could have been worse"; it is hard to imagine how. The total loss of money wagered has not yet been calculated, but it will be huge. Ross Wilson also stated that "of course" there will be a full investigation of the problems and these will be rectified so that it doesn't happen again.

Breakdowns of the TAB system on Melbourne Cup day have occurred before with the last major shutdown 4 years ago. Yesterday's problem was described as being the result of software modifications made to the TAB software 10 months prior to the Cup, and the excessive demand due to the huge increase in the number of bets activated a software bug in these modifications that lead to a shutdown of the system.

It is difficult to understand how the TAB system could not be designed and tested to accommodate the peak betting activity as the Melbourne Cup ALWAYS results in this level of high activity, and is therefore predictable and, you would imagine, able to be simulated. Agency owners, who are still trying to recover from the loss of income due to a protracted dispute with Sky Channel who supply direct TV coverage of horse racing, are now investigating legal action against the TAB.

Dr. Harley Mackenzie, Principal Operations Research Analyst,
Yallourn Energy
114 William Street Melbourne 3000, Australia +61 3 9207 7719
hjm@world.net

✦ Fidelity Brokerage computer problems

"George C. Kaplan" <gckaplan@cea.Berkeley.EDU>

Tue, 5 Nov 1996 17:00:49 -0800

An article in the **Wall Street Journal** 4 Nov 1996 describes a major problem

for Fidelity Brokerage Services (a discount stock brokerage) in London.

Very few details are given beyond "late bookings of dividends and other

problems", but it's serious enough that more than 50 people are working

14-hour days to sort through and correct three months of records **manually**.

British authorities have forced FBS to stop taking new customers until the problems are solved.

It appears to be a familiar story to RISKS readers: A new system was rushed into operation in April without adequate testing. FBS seems to be

in denial, claiming that the system wasn't rushed, but that they simply

"ran into some unanticipated glitches."

George C. Kaplan gckaplan@cea.berkeley.edu 510-643-5651

✦ Bug in the network: a real spider

+33)388412674 <"Nick BROWN " <Nick.BROWN@DCT.coe.fr> (Tel)>

18 Oct 1996 16:14:03 +0200

About five years ago we were the first on our block to have an Ethernet

segment implemented by a pair of 20 mW infra-red lasers. We had been promised that it was pretty reliable; as long as we could see the other

building, so could the laser.

And so it turned out; even though we spanned a canal in the foggiest town in France, we managed 98% uptime during the first few months (in the winter). Only on the foggiest days did we lose the connection, until about 10 each morning and from 4 each evening, for about 5 days total.

Came the spring, and we started to get breaks in the connection at what seemed to be random times. Eventually we worked out that it was happening half an hour after sunrise and half an hour after sunset. We thought it might be the sun in line with the laser, but the layout wasn't right for that. We changed every component in the network. Until...

One day, I noticed a spider's web connecting the laser box to the wall. Something must have flipped to On in my brain's background processing section, because about three days later (I run background processing on a very low priority), it dawned on me. I went up to the roof at the appropriate time and watched the laser carefully. Sure enough... a spider appeared, walked across the web, climbed into the transmission lens, and sat there (upside down), apparently eating its dinner, while a voice in my ear called "the link's down again !".

We got a cloth, a box of Q-tips, and an aerosol of insecticide, put them in a box marked "Network Hardware Maintenance Kit", and set up a weekly rota for cleaning the laser, and had no more problems. I dined out on the story for several months afterwards.

Nick Brown, Strasbourg, France (Nick.Brown@dct.coe.fr)

🔥 Announcement - Warning to Crypto and Banking Communities

Monty Solomon <monty@roscom.COM>

Wed, 6 Nov 1996 03:51:28 -0500

Begin forwarded message:

Date: Sun, 3 Nov 1996 18:16:37 -0500

To: coderpunks@toad.com

From: Ross Anderson <Ross.Anderson@cl.cam.ac.uk> (by way of Bruce Schneier)

Subject: Announcement - Warning to Crypto and Banking Communities

A serious weakness of DES

Draft - 2nd November 1996

Abstract

Eli Biham and Adi Shamir [[RISKS-18.56](#)] recently pointed out that if an attacker can induce unidirectional faults in key memory of cryptographic devices, then keys could be extracted quickly. Although their attack is very elegant, it is not practical against many fielded systems. For example, inducing a single-bit change in a DES key will cause a proper implementation to return a key parity error.

However, when combined with Peter Gutman's recent work on memory remanence, there are two very practical attacks. One of them allows smartcard electronic wallet keys to be extracted with much less expensive equipment than that currently used by pay-TV pirates; the other yields an effective attack against fielded banking security modules. These attacks show that a feature of DES that had long been thought innocuous is actually a serious design error.

Introduction

In a research announcement of 30th October, Biham and Shamir [[RISKS-18.54](#)]

point out that if a cryptographic hardware module employs EEPROM for key memory only, an opponent who can turn EEPROM values from `1' to `0' with a small controlled probability (e.g., by applying UV light) might cause a test input to be encrypted with a series of keys, each of Hamming distance one from the next in the series, and ending with the all zero key [1].

There are a number of reasons why their attack is not likely to work against real systems. For example, the typical smartcard system has several kilobytes of program code in EEPROM as well as typically two to five DES keys. An undirected stress applied to such a card is more likely to cause a program crash or an uninformative error than to yield a ciphertext encrypted under a key at Hamming distance one from a genuine key. Even if we only had to cause a hundred cards to fail to get a single input for the Biham-Shamir attack, if we needed on average 28 inputs to recover a DES key, then the number of cards required could be $O(100^{28})$.

The situation is made still worse by the fact that DES keys have odd parity, and a proper implementation will reject a key if any of its bytes has even parity. So one would be reduced to looking for keys at a Hamming distance of two rather than one. It is this objection that inspired the following work.

A Modified Attack

My idea is to turn the DES key parity problem on its head and enable parity to help rather than hinder the attack. Let us first consider an opponent who

can perform directed attacks on the chip. Reading the contents of an EEPROM cell directly is difficult, and people who do it for a living use focused ion beam workstations to modify the chip [2]. However, it is trivial to set an EEPROM cell to the value of your choice if you do not have to read it first; you only need two microprobes. A 10mS 18V pulse from the cell's source to its control gate will do the trick [3].

My modified attack therefore proceeds as follows. Set the first bit of the EEPROM containing the target DES key to 1 (or 0, the choice doesn't matter) and operate the device. If it still works, the keybit was a 1. If you get a 'key parity error' message, then the bit was zero. Move on to the next bit; set it to 1 and see if this changes the device's response (from encryption to error or vice versa).

This is a practical attack even on chips whose software we do not know in detail, as many smartcard software writers seem to have adopted a convention that the keys are located at the bottom end of the EEPROM memory. It will also work with protocols that use redundancy which we do not understand: we just change each key bit back to its original value.

The use of predictable memory addresses for keys is not restricted to smartcards; many banking security modules also keep keys at low memory. I will now describe a related attack that extracts master keys from these modules.

An Attack on Fielded Systems

In a brilliant Usenix paper [4], Peter Gutman described the mechanisms that

cause both static and dynamic RAM to `remember' values that they have stored for a long period of time. A prudent security engineer will ask what the effect of this is in the real world.

I looked at an instance of a security module used in banking. This security module has 12 pairs of DES master keys stored in low memory. The device is tamper resistant in that power to the key memory is cut when the box is opened for servicing (this is needed every few years to change the battery). Keys are loaded into the device afterwards in multiple components by trusted bank staff.

In this device, which dated from the late 1980's, the key values were substantially intact on power-up. The number of bits in error was of the order of 5-10%. I cannot give more accurate figures as I was not permitted to copy down either the correct master key values, nor the almost-correct values that had been `burned in' to the static RAM chips. I am also not permitted to name the bank at which these modules are installed, and it may not be prudent to name their manufacturer.

Nonetheless the crypto community should consider the consequences.

If each DES key is wrong by five bits, then the effort involved in searching for the 10 wrong bits in a double DES key might be thought to be 112-choose-10 operations. Each operation would involve (a) doing a 2-key 3DES decryption of a 64 bit PIN key whose enciphered value is widely known to the bank's programmers (b) in the 2^{-8} of cases where this result has odd parity, enciphering an account number with this as a DES key to see if the (decimalised) result is the corresponding PIN. The effort is 4

times

112-choose-10 DES operations - about 2^{50} . But it would probably be cheaper to do a hardware keysearch on the PIN key directly than to try to implement this more complex 2^{50} search in either hardware or software.

However, the bitwise nature of the DES key redundancy reduces the effort by orders of magnitude. If no key byte has a double error, then the effort is seven tries for each even parity byte observed, or 7^{10} - about 2^{28} , which is easy. If there is one key byte with a double error, the effort is 2^{38} , giving a search of 2^{40} DES operations - which is still feasible for an individual.

Conclusions

I have shown that the key parity in DES enables us to slash the cost of real attacks on both old systems (banking security modules) and new ones (electronic wallet smartcards).

I had already mentioned in [5] that a common fault in the driver software for banking security modules was that 'key parity error' messages were often ignored rather than copied to the bank's security manager to give warning of an attempted attack. This note shows that key parity is even more serious than that.

The nature of DES key redundancy now appears to be a design error; it would have been much better to calculate the redundancy on the whole key. The 16 bit MAC used in the Clipper and Capstone chips is preferable (although as shown in [6], 16 bits may not be enough to prevent some protocol attacks).

The lesson for bankers is that existing security modules (and other cryptographic devices) should be destroyed carefully at the end of their working life.

The lesson for security engineers is that we should add key redundancy, and the question of whether we can rely on a device's eventual destruction, to the growing list of system parameters that must be (a) explicitly considered during design and (b) examined carefully when the product is being evaluated.

Bibliography

- [1] ``The Next Stage of Differential Fault Analysis: How to break completely unknown cryptosystems'', Eli Biham, Adi Shamir, October 30th, 1996
 - [2] ``Tamper Resistance - A Cautionary Note'', Ross Anderson, Markus Kuhn, to appear at Usenix Electronic Commerce 96 (19th November)
 - [3] ``Hardwaresicherheit von Mikrochips in Chipkarten'', Osman Kocar, Datenschutz und Datensicherheit v 20 no 7 (July 96) pp 421--424
 - [4] ``Secure Deletion of Data from Magnetic and Solid-State Memory'', Peter Gutmann, Usenix Security 96 pp 77--89
 - [5] ``Why Cryptosystems Fail'', Ross Anderson, in Communications of the ACM v 7 no 11 (Nov 94) pp 32--40
 - [6] ``Protocol Failure in the Escrowed Encryption Standard'', Matt Blaze, in Proceedings of the 2nd ACM Conference on Computer and Communications Security (2-4 November 1994), ACM Press, pp 59--67
-

⚡ Differential Fault Analysis: a possible defence?

David R Brooks <daveb@iinet.net.au>

Wed, 06 Nov 1996 07:03:54 +0800

There has been much discussion lately, of the DFA attack on various cryptosystems. Defence strategies appear to be based on replication, either in space (dual-redundant crypto units, which check each other), or in time (do the crypto twice, and compare the results). Both techniques suffer from the same drawback: cost.

It occurs to me that a defence could be based on the use of RAM, rather than ROM or hardwired logic, to embody the crypto algorithm. In practical terms, this would mean a hardware embodiment using (say) a RAM-based FPGA, or a software system which would copy the code to RAM before execution. The point here is that there would be typically far more RAM bits used to specify the algorithm than are used to hold data-in-process. The odds are that an induced error will corrupt the operating code, rather than a data bit. The result will be either total garbage output, or the result of a "different" algorithm (the original, plus errors). Does this idea have any merit?

Dave Brooks <<http://www.iinet.net.au/~daveb>>

⚡ Ping o'Death from Windows 95

+33)388412674 <"Nick BROWN" <Nick.BROWN@DCT.coe.fr> (Tel)>

6 Nov 1996 17:18:18 +0000

Anybody with an Internet site, especially those without firewalls,

should
check out <http://www.sophist.demon.co.uk/ping/>. It details how
anybody with
Windows 95 and an IP address (hmmm, there might be one or two out
there...)
can crash a large range of network equipment (HP 3000, DEC Alpha, IBM
RS/6000, LaserJet printers, Netware servers, Windows PCs, routers,
etc),
apparently across the entire Internet.

Nick Brown, Strasbourg, France

🔥 Re: Office 97, VBA 5.0, and macro viruses (Slade, [RISKS-18.57](#))

Otto Stolz <Otto.Stolz@uni-konstanz.de>

Wed, 6 Nov 1996 17:26:40 +0000

Re: Slade in [RISKS-18.57](#) and VIRUS-L 9#208

Visual Basic is not the sole reason for these viruses to spread.

A virus needs three preconditions to spread:

- a platform that will execute its instructions,
- a vehicle in which it will be passed between users,
- a mechanism by which it will be executed unnoticed by the user.

For the Word macro viruses, the platform is the Word macro language.
VBA 5

will indeed make an upwards-compatible platform more widely
available.

However, Visual Basic is only sort of a syntactical framework: most
standard

functions and statements are only valid for a particular
application. (I do

not know VBA 5.0 yet, but I have coded a few macros both for Word
6.0 and

Excel 5.0 and found that the major part of the language were
application-specific, in both cases.) Hence, most VBA programs
probably will

only work with a particular application. So I think, we will not see
a much

more widely available platform for viruses to spread on, but rather

a couple
of similar, yet mutually almost incompatible platforms.

A platform in itself is no particular thread, virus-wise. Platforms are useful (after all, they are the sole purpose computers are built for). We should not worry about the proliferation of platforms, but rather on the other two preconditions for viruses to spread.

The vehicle for the Word macro viruses is Word templates disguised as documents. It was Microsofts greatest sin to allow Word templates (which contain the macros) to come disguised as documents. Word documents are widely, and frequently, exchanged amongst users. Now, if any document (according to the user's perception - even if it is, technically speaking, some other beast) can contain macros, this will constitute an ideal vector for macro viruses.

This is one of the two main reasons for Word macros to spread so rapidly. If the macros would be confined to separate files (as with most other applications), users would most probably leave the macros behind when giving away documents.

Word has two clandestine-execution mechanisms: macros with particular names (such as AutoOpen) are executed without explicit user action (e.g. when a document is opened) -- before the user even sees the document to be opened; macros with other particular names are bound to explicit user actions, such as hitting a button, or selecting a menu item. (If you think this is only one mechanism, you are probably right. No discussion on this triviality, please.)

In particular, the AutoOpen macro mechanism is the other main reason

for
Word macros to spread so rapidly: with this mechanism in place, a
user needs
only to **view** a Word document (e.g. an attachment of an e-mail
message, of
a news item, or of a WWW page) to contract a virus!

Conclusion: VBA 5.0 is not a particular threat, as long as the
applications
using it do not repeat Word's mistakes. Most important is to keep
macros
apart from application data (such as documents or spread-sheets);
second
most important is to avoid executing macros without the user's
consent.

Otto Stolz

✂ Web search engines find connected components

David Skillicorn <skill@qucis.queensu.ca>

Wed, 6 Nov 96 12:32:35 EST

The altavista search engine at least finds files that do not have
URLs
pointing to them, as long as they are in directories that it visits
for
other reasons. I discovered this when a search of a well-known CS
repository
turned up files containing all sorts of administrative information,
not
intended for public consumption.

It seems sensible to keep only things you want seen in directories
that web
servers can access. Having permissions set properly will prevent web
servers
seeing other files, but fouling up permissions is an easy error.

✂ **Re: Tote Board Crash at Breeder's Cup (Morphett, [RISKS-18.57](#))**

"Larry Kilgallen, LJK Software" <KILGALLEN@Eisner.DECUS.Org>

Tue, 05 Nov 1996 19:20:34 -0500 (EST)

I think there is a Risk in attempting to add the more robust features at the more shaky end of the language spectrum. Ada syntax (but not necessarily every implementation) supports unlimited programmer-specified ranges. That would seem a better starting place for programmer-unspecified ranges.

Anyone for zero-terminated integers ? :-)

Larry Kilgallen

✂ **Re: Tote Board Crash at Breeder's Cup (Morphett, [RISKS-18.57](#))**

Ian Rogers <ianr@cogs.susx.ac.uk>

Wed, 6 Nov 96 14:32 GMT

Perhaps you should check out Poplog Pop11. It is used mostly at research institutes, but also at some major process control sites where its garbage collection and wide range of number formats is highly valued.

Among its number formats are: fixed int, small float, double float, ratio (i.e. 10/3 is **not** approximated), imaginary (sqrt(-1) returns a sensible answer), and big ints (integers as big as the size of your VM -- one of the standard pop11 benchmarks is to calculate factorial(1000) :-)
Conversion between number formats is automatic in all the arithmetic functions.

Contact isl@isl.co.uk or comp.lang.pop
Ian Rogers, Sussex University

✉ Re: Tote Board Crash at Breeder's Cup (Morphett, [RISKS-18.57](#))

Henry G. Baker <hbaker@netcom.com>

Wed, 6 Nov 1996 08:07:34 -0800 (PST)

The Symbolics Lisp machine defaulted to 'infinite' (indefinite) precision integers. In fact, this property was inherited by other languages which ran on this machine, e.g., Fortran-77. 'Integers' in Symbolics Fortran would happily take on values like

378475974398573485743579875987495734987539759837594359749857398753475

Quoting from "User's Guide to FORTRAN 77 Tool Kit", August 1986:

"The Tool Kit supports arbitrary-precision integers, called `_bignums_`; as a result, all integers are immune from overflow..."

"The only operation for which arbitrary-precision integers are `_not_` valid is `_unformatted_` input/output. In this case, integers must be between -2^{31} and $2^{31}-1$."

"The Tool Kit detects uninitialized data (other than character data), so that an error condition results if a variable is used before it is assigned a value."

"The Symbolics Lisp Machine provides strong hardware data-type checking among logical, integer, and real data. Thus, the hardware prevents a program error due to equivalencing of the data, for example, in the case where the exponent and mantissa of a real number might be interpreted as an integer."

(I might point out that many of the standard Internet attacks which depend upon poor type or array bounds checking are worthless against such

machines;

I understand that they remained up and happily running, after many of their Unix brethren had been hopelessly compromised by Internet worms and other attacks.)

These significant advances in the quality of Fortran software was not appreciated by Fortran programmers, and the porting of existing Fortran programs -- which use such equivalencing very heavily -- became a nightmare.

However, the market was not kind to Symbolics, proving that software quality is not a particularly important feature in a computer system, as judged by paying customers.

✉ Re: -32768 (Brader, [RISKS-18.55](#))

Paul Eggert <eggert@twinsun.com>

Wed, 6 Nov 1996 11:32:37 -0800

Mark Brader's discussion of -32768 is correct as far as it goes, but it omits some of the more entertaining aspects of C expression evaluation.

Here's a table that may help RISKS readers appreciate some of the finer points.

This table uses the usual C notation: an ``0x'` prefix means hexadecimal; an ``L'` suffix means the type is ``long'`; ``U'` means ``unsigned'`. 2's complement arithmetic is assumed, so none of the expressions overflow. [SEE NOTE BELOW.] ``*'` marks disagreements with the usual mathematical meanings of expressions.

C expression	value of C expression, assuming:	
	16-bit `int`	32-bit `int`
32768	32768L	32768
0x8000	32768U	32768
-32767 - 1	-32768	-32768
-32768	-32768L	-32768
-0x8000	32768U *	-32768
-0x8000 == -32768	0 *	1
0U < -32767 - 1	1 *	1 *
0U < -32768	0	1 *
0 < -0x8000	1 *	0

Is everything clear now?

[NOTE added, at Mark Brader's suggestion: Paul's assumption is one that

is assumed for this posting only; it is not guaranteed by the language.

In particular, C can be legally implemented on 1's complement hardware,

where the value -32,768 is not permissible in a 16-bit int (or short)

at all. MB via PGN]

🔥 Re: -32768 (Fredriksson, [RISKS-18.57](#))

<Dik.Winter@cwil.nl>

Wed, 6 Nov 1996 14:39:35 GMT

What you are missing is that "-32768" in C is not a constant but an expression. The type of a C expression depends on the type of the operands and the operator. In this case the operand is "32768", the operator is "-".

The type of 32768 is "long" if the type "int" is only 16 bits, and so the

type of "-32768" is "long" in that case. But in the context of the definition of INT_MAX the type should be "int". On the other hand, when we write "-32767 - 1" the type is "int" because all constituent parts are of that type.

[This item is included to close the discussion off. Bear Giles had it

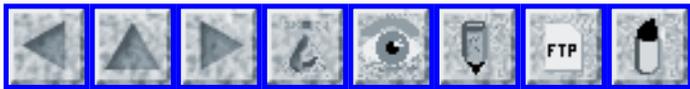
exactly right in his followup in [RISKS-18.49](#), and it might have been

better for me to have pointed that out privately to Kurt Fredriksson.

But the error is a common one, so perhaps it was worth flogging it once

more. Strong typing is the answer to a lot of questions, but it also

helps to understand the questions. 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 18: Issue 59

Thursday 7 November 1996

Contents

- [Intel product reaches directly into networked workstations](#)
[Jeff Mantei](#)
- [Big Internet is Watching You](#)
[Martin Minow](#)
- [Careful AeroPerusal](#)
[Peter Ladkin](#)
- [Risks of using keyless coinlockers in Vienna](#)
[Stefan Sachs](#)
- [Re: Fault-induced crypto attacks ...](#)
[Brian Randell](#)
- [Why cryptography is harder than it looks](#)
[Bruce Schneier](#)
- [Info on RISKS \(comp.risks\)](#)

✉ Intel product reaches directly into networked workstations

EDS OO/AI Svcs, Troy MI) <mantei@bbs.ug.eds.com (Jeff Mantei)>
Thu, 7 Nov 1996 13:35:48 -0800

I don't think this product or class of products has been mentioned in RISKS before, but I think their potential for abuse is self-evident and should be more widely known. I quote the following from:

http://www.intel.com/comm-net/sns/showcase/netmanag/ld_virus/whites/wp-etem.htm

"Intel is working to make the network's help desk more than just an answering service. With LANDesk Manager's remote access facility, network managers can take over a node and perform most of the tasks that typically would require a visit to the problem workstation.

"Under Novell's NMS, a network manager clicks on the node's network map object and launches LANDesk Manager's remote access tool. The manager can take over the user's PC and directly control the user's PC keyboard and mouse. The network manager can also access utilities and applications remotely, permitting checks of CONFIG.SYS, AUTOEXEC.BAT and WIN.INI files or anything else on the machine. This eliminates the laborious process of asking an end user to describe cryptic error messages and codes."

Big Internet is Watching You

Martin Minow <minow@apple.com>
Thu, 7 Nov 1996 07:29:32 -0800

Over the past month or so, a mailing list I subscribe to has endured a flame war with a disgruntled (ex-)subscriber. A few days ago, an

anonymous

participant provided what I'll call an Internet Biography of the subscriber.

The anonymous message began with "I had some free time this morning, and just for fun, thought I'd create a brief Net profile of our friend ..."

Among the discoveries are the following:

- Home address and phone number from <http://www.yahoo.com> (Four11 people search)
- Birthday from [http://www.boutell.com/birthday.cgi/\[Month\]/\[Day\]](http://www.boutell.com/birthday.cgi/[Month]/[Day])
- Company name and internet domain ownership from InterNIC.
- An uncomplimentary "who is ..." from a private academic site.
- A Usenet author profile showing over 500 messages posted to about 50 newsgroups over the last 18 months from <http://www.dejanews.com> profile.
- An uncomplimentary note from an academic, private "legends" homepage.
- Several professional contributions to FAQ's.

Over ten years ago, when computer bulletin boards appeared at my former employer, I formulated "Minow's law:" "never write anything you don't want to see on your resume." I seem to have been more prophetic than I expected.

Martin Minow, minow@apple.com

⚡ Careful AeroPerusal (Ladkin [RISKS-18.51](#), PGN [RISKS-18.57](#))

Peter Ladkin <ladkin@TechFak.Uni-Bielefeld.DE>

Fri, 8 Nov 1996 01:52:12 +0100

There are a lot of rumors about the latest AeroPeru news. CNN's

reports on
the latest AeroPeru findings have been inaccurate and
incomplete. PGN may
have helped to spread another one in [RISKS-18.57](#).

The facts are, from a source at the NTSB as well as information
about the
B757 static system (obtainable from my Compendium, see below):

- a) *Masking tape*, not duct tape or `Remove Before Flight'
Covers,
was covering the *left-side static ports* on the aircraft
[NTSB];
(there's no way to attach covers: the ports are flush with the
fuselage [B757 P/S system diagram]);
- b) Static ports to all three independent pitot-static systems
are on both
the left side and the right side of the fuselage, including
those for the
electro-mechanical backup: both static ports and pitot in each
system are
interconnected by an open tube [B757 pitot-static system
diagram];
- c) the right-side static ports have not been recovered; it is
therefore
not known whether masking tape was also covering these [NTSB];
- d) blockage of all the left static ports would cause some
degradation
of *all* the air data in both EFIS-displayed P/S systems plus
the backup;
blockage of the right-side static ports as well would cause
worse
degradation [general aero and system knowledge]; this is thus
a *common
failure mode* of all three independent P/S systems: both
primaries
and backup.
- e) the Peruvian Transport Ministry said that this obstruction of
the

sensors "could explain the erroneous and confusing altitude and speed information received by the pilots after takeoff" [NTSB source, quoting an official statement]. This contrasts with the Minister's reported statement on October 2 which seemed to the press to ascribe computer problems as the cause.

f) Putting masking tape on the ports when cleaning the aircraft is a normal maintenance procedure [NTSB]; however, leaving it on is certainly not! I don't know whether after such a procedure the aircraft has explicitly to be 'signed off' after inspection by a qualified inspector, who would then make a 'returned to service' entry in the maintenance logs. This is so for most procedures which render an aircraft temporarily unairworthy (as putting tape on the static ports does). This is a question still to be answered here, and I'm sure there are many readers who could do so;

g) A further question, posed by Jim Wolper, is why the air crew did not notice the tape on static ports on the pre-flight inspection.

It was dark, but nonetheless on most airplanes visually checking the static ports is an explicit item on the pre-flight inspection check list.

The B757 body is relatively high off the ground, but nevertheless I should have thought that tape on the ports would be clearly visible.

h) The CVR and DFDR have been recovered, examined in the NTSB Laboratories, and the data returned to Peruvian colleagues [NTSB];

In [RISKS-18.51](#), I expressed extreme scepticism that computer failure could be the sole cause of any B757 accident (except for one possibility which has never happened to any aircraft). It should now be clear that the recently-discovered failure mode under discussion is (a) not computer-related, and (b) deemed sufficient by itself to cause the known effects and history of the flight. This does not of course rule out other simultaneous failure modes that are computer-related. We still await the CVR and DFDR data.

More information about the B757 systems and about how a static-system blockage would affect the air data, as well as a history of the rather misleading statements and press reports about the AeroPeru accident, may be found (from Friday 8 November, 1996, and so dated) under the section on the AeroPeru accident in 'Computer-Related Incidents and Accidents to Commercial Airplanes', under <http://www.techfak.uni-bielefeld.de/~ladkin/> Until 8 November, information on the B757 pitot-static system may be found under the BirgenAir section.

Peter Ladkin

✦ Risks of using keyless coinlockers in Vienna

Stefan Sachs <ssachs@acm.org>

Thu, 31 Oct 1996 22:32:22 +-100

On my last trip to Vienna, I placed my baggage in a very advanced coinlocker

in an urban train station. The coinlocker uses a magnetic card instead of a conventional key. The user is guided by an LCD Screen on an operating panel serving six compartments (equipped with a numeric keypad, which is not used for normal operation). I received my card and since such cards are quite common in car parking facilities, left with confidence. On my way back, with only twenty minutes left for the train to the airport, following the instructions on the screen, I fed the card correctly positioned into the slot. Nothing happened and the screen continued to show the instruction, to feed the card into the slot to release the lock. When I asked at the ticket counter for help, the attendant was in no way astonished and explained that this happened because of children playing around with the keypad. A service technician was called and used the keypad to release the compartment lock, and then started a debugging session collecting several cards from the machine. Complaining that I needed my luggage, I was told that he already had made an 'exception' by handing me my suitcase without checking my identity and that it was my problem losing my card. Considering the need to reach my plane and the fact that I couldn't prove that I correctly inserted my card, I took my baggage and left.

The risks I see are these: If such a mechanism fails, it should in any case return the keycard it didn't accept. Since the keycard is not further protected by a PIN, it makes no sense to keep it to prevent abuse. Since the card is the only receipt, it is in the best interest of both,

the user and
the owner of the coinlocker, that it is always available.
Having a keypad,
which is obviously required only for servicing purposes open for
the public
is a completely unnecessary risk; sooner or later someone will
be successful
in opening the locker using the keypad. It is absolutely
irresponsible, to
continue to operate a system in which malfunction is so common
(during the
short time, I had to wait for the technician to open the locker,
two people
passing by told me, that they had experienced the same problems
before).

I can only recommend avoiding a coinlocker with such a setup,
under any
circumstances.

Dr. Stefan Sachs, Ringreiterweg 20, 23558 Luebeck, Germany +49-
451-8714936
ssachs@acm.org Dalbacka 30, 66600 Bengtsfors Sweden +46-
531-26069

⚡ Re: Fault-induced crypto attacks ... (Kocher, [RISKS-18.57](#))

Brian Randell <Brian.Randell@newcastle.ac.uk>
Wed, 6 Nov 1996 18:00:28 +0000

A different sort of fault, perhaps, but Tony Sale's lecture here
a few weeks
ago revealed that Bletchley Park's initial breaking of the Lorenz
teleprinter (a.k.a. "Fish") ciphers in the early years of WW2,
which led
subsequently to the building of the Colossus computers, was
entirely due to
one fault on the part of one German teleprinter operator. They
found that

he had resent one lengthy message, but by re-keying it (somewhat inaccurately) rather than using the punched teleprinter tape. From this one pair of messages they managed to discover the full detailed logical operation of the cipher machine unseen, and create a means of breaking the messages that were being sent using it to and from the German High Command. As Tony said, for the rest of the war, the cryptanalysts prayed that no over-eager Allied soldier captured a Fish machine!

Brian

PS. Years ago, after a lecture here by Donald Davies on DES, and emboldened merely by my reading of David Kahn and the like, I brought a typically-academic discussion of its security to a screeching halt by suggesting that perhaps sometime in the future I would be the proud possessor of a DES-based cipher machine -- which (like the Enigma cipher machine that I already own) was historically famous for the importance of the messages that machines like it had failed to protect. :-)

Dept. of Computing Science, University of Newcastle, Newcastle upon Tyne,
NE1 7RU, UK Brian.Randell@newcastle.ac.uk +44 191 222 7923

[And of course the Brits also invented E-fish-ient Chips. PGN]

⚡ Why cryptography is harder than it looks

Bruce Schneier <schneier@counterpane.com>
Wed, 6 Nov 1996 16:45:52 -0500

[The item originally in this place was intended to be a draft,

not a final

submission. I have removed it from the archive copy at Bruce's request.

The final version will appear in RISKS subsequently. 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 18: Issue 60

Friday 8 November 1996

Contents

- [Re: Why cryptography is harder than it looks](#)
[PGN](#)
- [Back In Time](#)
[Peter Wayner](#)
- [Risk of Earthquake Risk](#)
[Harold Asmis](#)
- [Mobile Phone Mayhem!](#)
[Trevor Warwick](#)
- ["NetLaw: Your Rights in the Online World" by Lance Rose](#)
[Rob Slade](#)
- [The final version of the NRC crypto report is now available!](#)
[Herb Lin](#)
- [Re: -32768 and strong typing](#)
[Jerry Leichter](#)
- [Re: Arbitrary precision arithmetic](#)
[Robert I. Eachus](#)
- [Re: Tote Board Crash at Breeder's Cup](#)
[Bear Giles](#)
[Mark Eichen](#)
- [Re: S-Bahn stopped by new switching software](#)

[Bob Frankston](#)

● [Call for papers: SafeComp'97](#)

[Bob Fields](#)

● [Info on RISKS \(comp.risks\)](#)

⚡ **Re: Why cryptography is harder than it looks (Schneier, [RISKS-18.59](#))**

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

Fri, 8 Nov 96 10:58:21 PST

I must apologize to Bruce for including a version of his thoughtful item in [RISKS-18.59](#) that he sent to the RISKS address that I mistakenly thought was his expected final version, but that was actually a draft in progress, sent for my information. As a consequence, I will be happy to run his final version whenever it is ready, and pardon your inconvenience for having to read two perhaps quite similar versions. Bruce has also asked me to ask you all to desist from redistributing copies around the net until the final version is ready.

⚡ **Back In Time**

Peter Wayner <pcw@access.digex.net>

Fri, 8 Nov 1996 12:51:07 -0500

Do you want to go back in time before the TWA 800 came down?

It's easy.

I've gotten in the habit of using Alta Vista to search the RISKS database

maintained in England on the web. Today, I was trying to dig up the old issue containing the story about the missile that took out a garage in British Columbia. So I sent this string:

```
+risks +neumann +vancouver +missile
```

The plus signs force Alta Vista to return documents that contain that word.

I've found that the word Risks and the name of our intrepid moderator is a great way to cut out the rest of the noise. This may be inefficient, but it is easier than remembering where a specific RISKS database is kept.

But the article didn't show up on the list. Surprisingly, there were a few other references. After some experimentation, I've discovered that the Alta Vista web crawler hasn't visited the UK website archive for some time. So the issue (18.40) wasn't included in its database.

The RISKS is that there is no easy way to tell how up-to-date Alta Vista may be. It may have indexed one region of the Net last night and another three months ago. I predict that this is another feature for web crawlers to work upon.

[I noted in an earlier issue ([RISKS-18.13](#)) that Alta Vista may still think

crvax.sri.com is the RISKS archive site rather than the up-to-date archive

at ftp.sri.com. I hope someone can finally fix that problem. The cutover

took place almost two years ago, but apparently the old crvax archives are

STILL in place and they include only issues up to [RISKS-16.64](#). PGN]

⚡ Risk of Earthquake Risk

Harold Asmis <harold.w.asmis@hydro.on.ca>

Thu, 07 Nov 1996 14:01:29 -0500

Last week, the new California Earthquake Insurance agency announced that they would shortly be releasing a billion dollars worth of Earthquake bonds, which pay diminished returns if there is a major California earthquake. This step was necessary because most insurers are pulling out of California earthquake insurance, due to the inadequacy of reserves. We wonder about the RISK of a state-run insurance agency locating all its computers and staff (for payouts and bond administration) in the very state the flattening of which would trigger these bonds and payouts.

Harold W. Asmis
416.592.7379

harold.w.asmis@hydro.on.ca tel

⚡ Mobile Phone Mayhem!

"Trevor Warwick INF-SP" <twarwick@madge.com>

Thu, 7 Nov 96 17:18:26 -0000

Another twist on the well known "Cleaner buffs computer room floor and takes down entire site" stories:

We recently had some engineers from AT&T in our computer room for three days, working on a PABX which also lives in there. During this period, two of our main Netware servers have been extremely unreliable,

crashing several
times a day. The AT&T engineers were working near these servers,
and we
initially thought that they might have been causing the crashes
by
disturbing some cables.

After a few of these unexplained crashes, one of our MIS group
noticed that
every time he went in to the server room to reboot the dead
servers, one of
the AT&T engineers was using his mobile phone. So, they were
asked to turn
their phones off while working in the server room, and the
problem has not
reoccurred.

To test the theory a bit further, the MIS group then took an
otherwise
unused server, and experimented with using a mobile phone near
it. With the
working phone being used less than a foot away from the machine,
they
provoked a crash which corrupted the system disk (and its mirror
volume)
beyond repair.

Trevor Warwick, Madge Networks, Sefton Park, Bells Hill, Slough,
England
+44 (0)1753 661401 twarwick@madge.com fax : +44 (0)1753
661011

✦ "NetLaw: Your Rights in the Online World" by Lance Rose

Rob Slade <roberts@mukluk.hq.decus.ca>
Wed, 06 Nov 1996 14:00:37 EST

BKNETLAW.RVW 950406

"NetLaw: Your Rights in the Online World", Lance Rose, 1995, 0-

07-882077-4,

U\$19.95

%A Lance Rose

%C 2600 Tenth St., Berkeley, CA 94710

%D 1995

%G 0-07-882077-4

%I McGraw-Hill

%O U\$19.95 510-548-2805 800-227-0900 lkissing@osborne.mhs.
compuserve.com

%O pmon@osborne.mhs.compuserve.com

%P 372

%T "NetLaw: Your Rights in the Online World"

Very similar to his earlier "Syslaw" (cf. BKSYSLAW.RVW), this is a general guide to various legal aspects of life online. The major changes are the broadening of the scope from BBS level systems to include online services and the Internet, and very handy (and interesting) sidebars, which give a thumbnail sketch version of the topic under discussion. These usually include a reference to some specific case.

Chapters address the issues of censorship, contracts, commerce, and copyright. Chapter four, which deals with the responsibility of the system operator in light of online dangers, does touch on the topic of malicious software. I was disappointed that this is limited to a not terribly accurate defining of terms, and almost no discussion of the admittedly confused legal situation. Further chapters cover privacy, crime, search and seizure, and a rather disappointing chapter on obscenity. Appendices include some very useful sample contracts, and various US laws.

Given recent developments which have strongly indicated the international

nature of the net and international legal ramifications, it is discouraging to see that Rose still presents only a limited and US-centric view. However, the general principles he describes are held in common law, and this book should at least provide guidance for the broader online world.

copyright Robert M. Slade, 1995 BKNETLAW.RVW 950406

Vancouver Institute for Research into User Security Canada V7K 2G6

ROBERTS@decus.ca Robert_Slade@sfu.ca rslade@cyberstore.ca
rslade@sfu.ca

⚡ The final version of the NRC crypto report is now available!

"CRYPTO" <crypto@nas.edu>

Fri, 08 Nov 96 15:28:00 EST

The Computer Science and Telecommunications Board (CSTB) of the National Research Council (NRC) is pleased to announce the availability of its cryptography policy study "Cryptography's Role in Securing the Information Society". This report was originally released in pre-publication form on May 30, 1996.

The final printed version of this report can be obtained from the National Academy Press, 1-800-624-6242 or Web site <http://www.nap.edu/bookstore>. The pre-publication version and the final printed copy differ in that the printed copy contains an index and many source documents relevant to the crypto policy debate; of course, editorial corrections have been

made as
well.

An unofficial ASCII version of the prepublication report can be found at <http://pwp.usa.pipeline.com/~jya/nrcindex.htm>; the official NRC version should become available online in ASCII form in December.

In addition, CSTB has been conducting briefings on this report at various sites around the country; if you would like to arrange a briefing in your area, please let us know (cstb@nas.edu, 202-334-2605).

[Message from Herb Lin]

[I note that when we held a briefing on the West Coast, Herb was surprised to find that a scanned copy of the original report had already appeared on-line, shortly after the draft report had been released. The final version is over 700 pages with all the appendices. But I suspect that an unofficial on-line version of the official report may not be far behind -- despite its copyright. Incidentally, the full report is an extraordinary source of background material. PGN]

⚡ Re: -32768 and strong typing

Jerry Leichter <leichter@lrw.com>
Thu, 7 Nov 96 00:33:42 EDT

Just when you thought everything there was to be said about this issue had already been said, our esteemed moderator commented that "Strong

typing is the answer to a lot of questions, but it also helps to understand the questions".

Unfortunately, strong typing is **not** the answer to this particular question!

Niklaus Wirth probably deserves to be considered the inventor of strong typing with his development of Pascal. (The idea was probably around earlier, but no one talked about it much until Pascal's advantages and faults were under discussion.) Pascal had no unsigned type, so the question at hand didn't arise.

Wirth next designed the Modula and Modula-2 languages. I don't know much about Modula, but Modula-2 has both INTEGER (C int) and CARDINAL (C unsigned) types. Modula-2 is strongly typed, and has no implicit conversions. It isn't possible to mix INTEGER's and CARDINAL's in an expression. (You can, of course, include explicit type conversions.) This avoids all the complexities and ambiguities that occur in C when signed and unsigned types "meet across an operator". So, indeed, our moderator is correct: Strong typing helps.

However, the problem of constants remains. Modula-2 does not have an explicit "unsigned constant" marker; integral constants are just strings of digits. (By the way, Modula-2, like C, considers -1234 to be the unary minus operator applied to the constant 1234.) What type should be assigned to integral constants? Choosing either INTEGER or CARDINAL causes problems since then

it becomes impossible to, say, compare a CARDINAL or INTEGER to a constant value without an explicit conversion. The *intent* all along has been that integer constants should take on "the right" type; but getting that defined right turned out to be unexpectedly difficult. (-1234 ought to be INTEGER, never a CARDINAL - but it's not a constant, it's an expression. If we say that the result of negation is always an INTEGER, then --1234 and 1234 have different types - rather annoying. And how about -0? Do we have to assume constant folding as part of the language definition? And so on, and so on.)

Modula-2 was officially defined by Wirth's book, "Programming in Modula-2", which went through four editions. Each edition contained changes to the language definition. I believe that the details of the treatment of constants changed with each edition. There is currently an ISO draft standard for Modula-2; it uses an entirely different approach for defining the semantics of integral constants, in yet another attempt to get at the "obvious" meaning. (The standard, as I understand it, assigns an abstract "NUMBER" type to constants. Unlike actual types, this abstract type *can* be automatically coerced - to INTEGER or CARDINAL, as the case may be. The details of this abstract type then need to be worked out....)

So strong typing didn't help quite enough.

It's instructive to consider yet another language, Modula-3. Modula-3 was developed at DEC SRC by a number of people, with consultation and review

from Wirth. Like Modula-2, Modula-3 has types called INTEGER and CARDINAL.

Like Modula-2, Modula-2 is strongly typed. However, Modula-3 chose to avoid the entire issue of the typing of integral constants, and all other questions about how signed and unsigned values interact, by defining CARDINAL differently: In Modula-3, CARDINAL is simply the non-negative members of the INTEGER type.

Now, one reason Modula-3 was able to do this is that it pretty much assumes 32-bit integers. With 16-bit integers, there was often good reason to want to use unsigned values simply to expand the range of counters and such. With 32-bit integers, that's hardly ever worth the effort.

By the way, for those who might object that there are legitimate uses for true unsigned arithmetic: Modula-3 actually provides that, in the form of a required interface that defines a WORD type and various operations on it. WORD is in fact a synonym for integer, but the operations treat WORDS as unsigned values.

Sometimes the right solution is not to trim the leaves but to pull the weed out by its roots. To those of us who programmed on 16-bit machines - including, it seems, Niklaus Wirth - it takes a bit of effort to realize that the tricks we had to use to get enough range out of our integers simply are no longer needed, and there's no longer a need to distort our languages to try to support them. But that's clearly the way to sanity.

-- Jerry

✂ Re: Arbitrary precision arithmetic (Kilgallen, [RISKS-18.58](#))

"Robert I. Eachus" <eachus@spectre.mitre.org>

Thu, 7 Nov 1996 21:38:31 -0500

Actually every Ada compiler supports arbitrary precision arithmetic--at compile time. Static integer constants are required to be evaluated without overflow, and the easiest way to guarantee this is to evaluate them using an arbitrary precision arithmetic package.

Most compiler vendors use a package written over a decade ago by Gerry Fisher, and almost all of them make it available to users as well. Of course this requirement has its disadvantages, a early "bug" in many Ada compilers was that type declarations like:

```
type My_Int is range 0..2**Integer'Last - 1;
```

Took a VERY long time to be rejected. (Dave Emery discovered this problem by accident. He intended to write 2**Integer'Length...)

✂ Re: Tote Board Crash at Breeder's Cup ([RISKS-18.56,57](#))

Bear Giles <bear@indra.com>

Thu, 7 Nov 1996 10:29:16 -0700

There are numerous implementations of indefinite-precision arithmetic in C (e.g., the Gnu "mp" package); several of these have been

encapsulated into
strong C++ classes. Implementations include both a (very large)
fixed-sized
array and a malloc'd array.

Unfortunately, there are several problems with these packages:

- speed (compared to "regular" integers),
- file I/O is much more difficult when you don't know how long your integers can be, and
- ITAR restrictions on export of munitions.

The last point isn't a mistype -- I'm not an unbiased observer, but every implementation I've seen has been part of a cryptographic package... and once you have a good indefinite-precision arithmetic package it's trivial to implement many cryptographic protocols.

Bear Giles bear@indra.com

⚡ Re: Tote Board Crash at Breeder's Cup (Morphett, [RISKS-18.57](#))

Mark Eichen <eichen@cygnus.com>

06 Nov 1996 14:58:05 -0500

> To my mind they are as silly as bugs which arise in programmes because of
> fixed length strings, such as the famous one in sendmail where it didn't
> check the size of a string it was strcpy'ing into a fixed length buffer.

Point of information: the fixed length buffer was in "fingerd", not sendmail. sendmail had a much more obvious problem (a "DEBUG" function that was not removed in production.) It was noted that

the
problem (using the unsafe "gets" function) was tiresome even
then...

(See <http://www.mit.edu/people/eichin/virus/main.html> for more
details

than most people would ever want, or CACM 6/89, or IEE S&P
5/1/89.)

⚡ Re: S-Bahn stopped by new switching software (Weber-Wulff, [RISKS-18.55](#))

<Bob_Frankston@frankston.com>

Fri, 8 Nov 1996 14:02 -0500

We have ways of assuring that software won't fail? Please
enlighten me. We
have ways of reducing the likelihood. But assuring?

I too am happy that no one got killed, the rest is a detail.

OK, to be fair, the getting the same naive error in a second
implementation
does sound inexcusable but we should confuse the inability to
simulate the
complete real-time operation (or even, the failure to do so)
with the gross
error of ignoring a known critical bug. This is not about
assurance but, if
true, about incompetence.

[Also commented on by Mark Stalzer, mas@acm.org. PGN]

⚡ Call for papers: SafeComp'97

<bob@minster.cs.york.ac.uk>

Call for Papers

SAFECOMP '97

The 16th International Conference on
Computer Safety, Reliability and Security

University of York, UK

September 8th-10th, 1997

Sponsored by EWICS TC 7

European Workshop on Industrial Computer Systems Technical
Committee 7

SAFECOMP is an annual event reviewing the state of the art, experiences and new trends in the areas of computer safety, reliability and security. The conference focuses on critical computer applications. It is intended to form a platform for technology transfer between academia, industry and research institutions.

Papers are invited on all aspects of computer systems in which safety, reliability and security are important. Industrial sectors include, but are not restricted to, avionics, space industry, railway and road transportation, process industry, automotive industry, and research.

Papers due by 1 Feb 1997.

For more information on the conference, the full call for papers, and submission instructions visit our world wide web site at:

<http://www.cs.york.ac.uk/safecomp-97>

or contact:

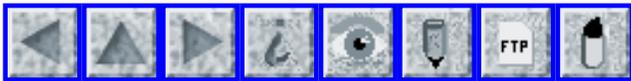
Ginny Wilson, SAFECOMP '97, Department of Computer Science,
University of York

York, YO1 5DD, UK Tel: + 44 1904 432782 Fax: + 44 1904
432708

Email: safecomp-97@minster.york.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 18: Issue 61

Friday 15 November 1996

Contents

- [San Jose garbage billing system snafu](#)
[PGN](#)
- [Revealing Software Glitch Bares Credit Card Info on the Web](#)
[Edupage](#)
- [Good Java security doesn't imply good network security](#)
[David Martin](#)
- [Making good ActiveX controls do bad things](#)
[Richard M. Smith](#)
- [Invention by Design, Henry Petroski](#)
[PGN](#)
- [Compile-time checking](#)
[Arthur Marsh](#)
- [Eastern what time?](#)
[Mark Brader](#)
- [Why Cryptography is Harder than it Looks](#)
[Bruce Schneier](#)
- [Risks in cryptography advertising](#)
[Gene Berkowitz](#)
- [Info on RISKS \(comp.risks\)](#)

⚡ San Jose garbage billing system snafu

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

Fri, 15 Nov 1996 13:15:16 PST

San Jose, California, has issued no garbage bills (186,000 homes and 3765 apartments) since the beginning of October -- because of ``faulty procedures in saving backup records.' ' The city is spending \$360,000 to rectify the situation, which will take another month. [Source: *San Jose Mercury News*, 13 Nov 1996, courtesy of Babak Taheri.] Garbage collections continue, while revenue collections do not. GOGIgigo = Garbage Out, Garbage In, garbage in, garbage out (with respect to real and virtual garbage, respectively).

⚡ Revealing Software Glitch Bares Credit Card Info on the Web

Edupage Editors <educom@elanor.oit.unc.edu>
Sun, 10 Nov 1996 16:42:03 -0500 (EST)

Some Web shoppers have recently had their worst fears about electronic commerce confirmed -- the credit card information they trustingly typed in was accessible by anyone using a simple Web browser. The sites affected had improperly installed a software program called SoftCart, made by Mercantec Inc., to handle their transactions. "Our standard documentation clearly explains how to avoid these security break-ins," says Mercantec's president. The problem was attributed to human error, which occurred when inexperienced installers failed to place completed order forms in directories not accessible to Web browsers. Vendors affected by the glitch say they've taken steps to remedy the situation. (*Wall Street Journal*, 8 Nov 1996, B6)

⚡ Good Java security doesn't imply good network security

David Martin <dm@cs.bu.edu>
15 Nov 1996 15:24:20 -0500

Many researchers have noted security flaws in existing Java implementations as well as fundamental weaknesses in Java's security model. Examples of the former include attacks that confuse Java's type system, ultimately allowing applets to execute arbitrary code with the full permission of the user invoking the browser, and examples of the latter include the lack of audit trails and Java's single-line-of-defense strategy. Dean, Felten, and Wallach's paper "Java Security: From HotJava to Netscape and Beyond" brought most of these issues to light, sending shock waves throughout the computing community. (See <http://www.cs.princeton.edu/sip>).

Until now users and system designers have been content to consider these

problems transient, confident that bugs will be mended quickly enough to limit any damage. Netscape, for instance, has been admirably quick in responding to the most serious problems.

However, the giant installed base of Java-enabled browsers---each inviting an adversary to determine the browser's actions---gives reason to suspect some kind of fallout even in "secure" implementations of Java. Our paper, available at <http://www.cs.bu.edu/techreports/96-026-java-firewalls.ps.Z>, describes attacks on firewalls that can be launched from legal Java applets. In certain firewall environments, a Java applet that finds itself running in a browser behind the firewall can cause the firewall to allow incoming telnet (or other TCP) connections to that host. In some cases, the applet can even use the firewall to access arbitrary hosts supposedly protected by the firewall.

The weaknesses exploited by these attacks are neither in the Java implementation nor in the firewall as such, but rather in the composition of the two---and in the security model that results when browsers give adversaries such ready access to "protected" hosts.

Our paper also describes methods for preventing applets from crossing a firewall; this is one way to prevent such attacks. In any case we strongly recommend that managers of firewalled sites containing Java-enabled browsers take a good look at the issues involved and make appropriate policy decisions.

David Martin <dm@cs.bu.edu>, Computer Science, Boston University
Sivaramakrishnan Rajagopalan <sraj@bellcore.com>, Bellcore
Avi Rubin <rubin@bellcore.com>, Bellcore

⚡ Making good ActiveX controls do bad things

"Richard M. Smith" <rms@pharlap.com>
Mon, 11 Nov 1996 23:49:03 -0500

There has been a great deal of talk about how ActiveX controls can be written to do malicious things on the Internet. However, what has not been recognized is that even standard ActiveX controls can be made to do malicious things via HTML and VBScript. Here are two simple examples of "good" ActiveX controls being made to do "bad" things:

The computer crashing URL - `file:///aux`

If Microsoft's ActiveMovie control is told to play a movie from the URL `file:///aux` Internet Explorer will go into an infinite loop under Windows 95. Attempting to shutdown Internet Explorer by doing an "End

Task" will more often than not crash Windows 95. This bug can be exploited by the "bad guys" to create HTML pages that will crash people's computers when the pages are downloaded from a web site.

VBScript and ActiveX combo disk crasher

Even more worrisome are ActiveX controls that contain methods (i.e., function calls) that write files to disks. These methods can be used by a simple VBscript program to overwrite key system files like AUTOEXEC.BAT, CONFIG.SYS, REG.DAT etc. The damage is done simply by viewing an HTML page that contains the ActiveX control and the malicious VBScript code. I know of at least three commercially available ActiveX controls that have methods that will save files to disk. Any of these controls, I believe, can be exploited to build a disk crash HTML page. At least two of these controls have valid Authenticode digital signatures so that they can be automatically downloaded and executed even with the highest security settings in Internet Explorer 3.

The big question in my mind is what can be done about solving these sorts of ActiveX security problems.

Richard Smith

Invention by Design, Henry Petroski

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

Mon, 28 Oct 96 9:57:08 PST

Well, one of our old-favorite sources of RISKS quotes has done it again!

Henry Petroski

Invention by Design: How Engineers Get from Thought to Thing

Harvard University Press, Cambridge, Massachusetts

November 1996, 288 pages. ISBN 0-674-46367-6

This book explores the underlying essence of engineering -- not so much what makes particular products tick (or not tick), but rather why is it that the process of engineering design can evolve so successfully (or unsuccessfully, as the case may be). The chapters range widely over paper clips, pencils, zippers, aluminum cans, faxes and networks, planes and computers, water and society, bridges and politics, and finally buildings and systems. It has long been my contention that those of us involved in developing and using computer systems have much to learn from the more traditional engineering disciplines. Henry himself modestly eschews analysis of computer system

developments and computer engineering, perhaps because there are fundamental differences between his disciplines and our "discipline" (or lack thereof). He typically leaves it to us to bridge the gap. However, this book provides us with an excellent step in that direction.

✦ Compile-time checking (re: Eachus, [RISKS-18.60](#))

<arthur@gateway.dircsa.org.au>

Tue, 12 Nov 96 16:17 CST

Robert I. Eachus <eachus@spectre.mitre.org> wrote in [RISKS-18.60](#):

"Actually every Ada compiler supports arbitrary precision arithmetic--at compile time. Static integer constants are required to be evaluated without overflow, and the easiest way to guarantee this is to evaluate them using an arbitrary precision arithmetic package."

I had an integer constant evaluate **with** overflow during this past week.

Whilst updating a DNS record, I accidentally set the serial number to 19961100808, when it should have been 1996110808, corresponding to the four digit year, two digit month and two digit hour of the day.

When checking the DNS record from the name daemon using nslookup (which is essentially viewing a run-time interpretation of the DNS record), the serial number looked nothing like what was entered in the DNS record. The serial number had been evaluated, overflowed and the truncated result was being used, without any complaint from the name daemon when it had re-loaded the DNS record. As DNS serial numbers have to always increase for updates to propagate, and I wanted something that wouldn't overflow, I ended up using 2996111117 as the new serial number.

As an accidental increase of a DNS serial number cannot be easily rectified, I believe that the name daemon should have refused to load the DNS record with a serial number that would cause an overflow.

Arthur Marsh, tel +61-8-8370-2365, fax +61-8-8223-5082 arthur@dircsa.org.au

✦ Eastern what time? (Leichter, [Risks-18.60](#))

Mark Brader <msb@sq.com>

Wed, 13 Nov 96 12:27:52 EST

As I was looking at Jerry Leichter's article about "-32768 and strong typing", I was surprised to notice that it appeared under the line:

Date: Thu, 7 Nov 96 00:33:42 EDT

As North American readers know, daylight saving time in the USA (where Jerry's site is located) ended for the year on October 27. So should we take this as "Wed, 6 Nov 96 23:33:42 EST", or "Thu, 7 Nov 96 00:33:42 EST", or something else? And is there an interesting reason why it was wrong?

Mark Brader msb@sq.com SoftQuad Inc., Toronto

⚡ Why Cryptography is Harder than it Looks [LONG]

Bruce Schneier <schneier@counterpane.com>

Mon, 11 Nov 1996 15:37:42 -0500

[This version completely supersedes the earlier draft that inadvertently appeared in [RISKS-18.59](#). PGN]

WHY CRYPTOGRAPHY IS HARDER THAN IT LOOKS
Bruce Schneier, Counterpane Systems

.....
Copyright Nov 1996 by Bruce Schneier. All rights reserved. Permission is given to distribute this essay, providing that it is distributed in its entirety (including this copyright notice). For more information on Counterpane Systems's cryptography and security consulting, see <http://www.counterpane.com>. [The intent of this notice is stronger than the default RISKS policy: This piece may be freely reproduced in its entirety, but only in its entirety without modification, including this banner and Bruce's final line of identifying information. By RISKS policy, such reproduced copies should also bear the relevant RISKS masthead identification:

Risks-Forum Digest (comp.risks) Friday 15 November 1996 Volume 18 Issue 61
.....

>From e-mail to cellular communications, from secure Web access to digital cash, cryptography is an essential part of today's information systems. Cryptography helps provide accountability, fairness, accuracy, and confidentiality. It can prevent fraud in electronic commerce and assure the validity of financial transactions. It can prove your identity or protect your anonymity. It can keep vandals from altering your Web page and prevent industrial competitors from reading your confidential documents. And in the future, as commerce and communications continue to move to computer

networks, cryptography will become more and more vital.

But the cryptography now on the market doesn't provide the level of security it advertises. Most systems are not designed and implemented in concert with cryptographers, but by engineers who thought of cryptography as just another component. It's not. You can't make systems secure by tacking on cryptography as an afterthought. You have to know what you are doing every step of the way, from conception through installation.

Billions of dollars are spent on computer security, and most of it is wasted on insecure products. After all, weak cryptography looks the same on the shelf as strong cryptography. Two e-mail encryption products may have almost the same user interface, yet one is secure while the other permits eavesdropping. A comparison chart may suggest that two programs have similar features, although one has gaping security holes that the other doesn't. An experienced cryptographer can tell the difference. So can a thief.

Present-day computer security is a house of cards; it may stand for now, but it can't last. Many insecure products have not yet been broken because they are still in their infancy. But when these products are widely used, they will become tempting targets for criminals. The press will publicize the attacks, undermining public confidence in these systems. Ultimately, products will win or lose in the marketplace depending on the strength of their security.

THREATS TO COMPUTER SYSTEMS

Every form of commerce ever invented has been subject to fraud, from rigged scales in a farmers' market to counterfeit currency to phony invoices. Electronic commerce schemes will also face fraud, through forgery, misrepresentation, denial of service, and cheating. In fact, computerization makes the risks even greater, by allowing attacks that are impossible against non-automated systems. A thief can make a living skimming a penny from every Visa cardholder. You can't walk the streets wearing a mask of someone else's face, but in the digital world it is easy to impersonate others. Only strong cryptography can protect against these attacks.

Privacy violations are another threat. Some attacks on privacy are targeted: a member of the press tries to read a public figure's e-mail, or a company tries to intercept a competitor's communications. Others are broad data-harvesting attacks, searching a sea of data for interesting information: a list of rich widows, AZT users, or people who view a particular Web page.

Electronic vandalism is an increasingly serious problem. Computer vandals have already graffitied the CIA's web page, mail-bombed Internet providers, and canceled thousands of newsgroup messages. And of course, vandals and thieves routinely break into networked computer systems. When security

safeguards aren't adequate, trespassers run little risk of getting caught.

Attackers don't follow rules; they cheat. They can attack a system using techniques the designers never thought of. Art thieves have burgled homes by cutting through the walls with a chain saw. Home security systems, no matter how expensive and sophisticated, won't stand a chance against this attack. Computer thieves come through the walls too. They steal technical data, bribe insiders, modify software, and collude. They take advantage of technologies newer than the system, and even invent new mathematics to attack the system with.

The odds favor the attacker. Bad guys have more to gain by examining a system than good guys. Defenders have to protect against every possible vulnerability, but an attacker only has to find one security flaw to compromise the whole system.

WHAT CRYPTOGRAPHY CAN AND CAN'T DO

No one can guarantee 100% security. But we can work toward 100% risk acceptance. Fraud exists in current commerce systems: cash can be counterfeited, checks altered, credit card numbers stolen. Yet these systems are still successful because the benefits and conveniences outweigh the losses. Privacy systems -- wall safes, door locks, curtains -- are not perfect, but they're often good enough. A good cryptographic system strikes a balance between what is possible and what is acceptable.

Strong cryptography can withstand targeted attacks up to a point -- the point at which it becomes easier to get the information some other way. A computer encryption program, no matter how good, will not prevent an attacker from going through someone's garbage. But it can prevent data-harvesting attacks absolutely; no attacker can go through enough trash to find every AZT user in the country. And it can protect communications against non-invasive attacks: it's one thing to tap a phone line from the safety of the telephone central office, but quite another to break into someone's house to install a bug.

The good news about cryptography is that we already have the algorithms and protocols we need to secure our systems. The bad news is that that was the easy part; implementing the protocols successfully requires considerable expertise. The areas of security that interact with people -- key management, human/computer interface security, access control -- often defy analysis. And the disciplines of public-key infrastructure, software security, computer security, network security, and tamper-resistant hardware design are very poorly understood.

Companies often get the easy part wrong, and implement insecure algorithms and protocols. But even so, practical cryptography is rarely broken through the mathematics; other parts of systems are much easier to break. The best protocol ever invented can fall to an easy attack if no one pays

attention to the more complex and subtle implementation issues. Netscape's security fell to a bug in the random-number generator. Flaws can be anywhere: the threat model, the system design, the software or hardware implementation, the system management. Security is a chain, and a single weak link can break the entire system. Fatal bugs may be far removed from the security portion of the software; a design decision that has nothing to do with security can nonetheless create a security flaw.

Once you find a security flaw, you can fix it. But finding the flaws in a product can be incredibly difficult. Security is different from any other design requirement, because functionality does not equal quality. If a word processor prints successfully, you know that the print function works. Security is different; just because a safe recognizes the correct combination does not mean that its contents are secure from a safecracker. No amount of general beta testing will reveal a security flaw, and there's no test possible that can prove the absence of flaws.

THREAT MODELS

A good design starts with a threat model: what the system is designed to protect, from whom, and for how long. The threat model must take the entire system into account -- not just the data to be protected, but the people who will use the system and how they will use it. What motivates the attackers? Must attacks be prevented, or can they just be detected? If the worst happens and one of the fundamental security assumptions of a system is broken, what kind of disaster recovery is possible? The answers to these questions can't be standardized; they're different for every system. Too often, designers don't take the time to build accurate threat models or analyze the real risks.

Threat models allow both product designers and consumers to determine what security measures they need. Does it make sense to encrypt your hard drive if you don't put your files in a safe? How can someone inside the company defraud the commerce system? How much would it cost to defeat the tamper-resistance on the smart card? You can't design a secure system unless you understand what it has to be secure against.

SYSTEM DESIGN

Design work is the mainstay of the science of cryptography, and it is very specialized. Cryptography blends several areas of mathematics: number theory, complexity theory, information theory, probability theory, abstract algebra, and formal analysis, among others. Few can do the science properly, and a little knowledge is a dangerous thing: inexperienced cryptographers almost always design flawed systems. Good cryptographers know that nothing substitutes for extensive peer review and years of analysis. Quality systems use published and well-understood algorithms and protocols; using unpublished or unproven elements in a design is risky at best.

Cryptographic system design is also an art. A designer must strike a balance between security and accessibility, anonymity and accountability, privacy and availability. Science alone cannot prove security; only experience, and the intuition born of experience, can help the cryptographer design secure systems and find flaws in existing designs.

IMPLEMENTATION

There is an enormous difference between a mathematical algorithm and its concrete implementation in hardware or software. Cryptographic system designs are fragile. Just because a protocol is logically secure doesn't mean it will stay secure when a designer starts defining message structures and passing bits around. Close isn't close enough; these systems must be implemented exactly, perfectly, or they will fail. A poorly-designed user interface can make a hard-drive encryption program completely insecure. A false reliance on tamper-resistant hardware can render an electronic commerce system all but useless. Since these mistakes aren't apparent in testing, they end up in finished products. Many flaws in implementation cannot be studied in the scientific literature because they are not technically interesting. That's why they crop up in product after product. Under pressure from budgets and deadlines, implementers use bad random-number generators, don't check properly for error conditions, and leave secret information in swap files. The only way to learn how to prevent these flaws is to make and break systems, again and again.

CRYPTOGRAPHY FOR PEOPLE

In the end, many security systems are broken by the people who use them. Most fraud against commerce systems is perpetrated by insiders. Honest users cause problems because they usually don't care about security. They want simplicity, convenience, and compatibility with existing (insecure) systems. They choose bad passwords, write them down, give friends and relatives their private keys, leave computers logged in, and so on. It's hard to sell door locks to people who don't want to be bothered with keys. A well-designed system must take people into account.

Often the hardest part of cryptography is getting people to use it. It's hard to convince consumers that their financial privacy is important when they are willing to leave a detailed purchase record in exchange for one thousandth of a free trip to Hawaii. It's hard to build a system that provides strong authentication on top of systems that can be penetrated by knowing someone's mother's maiden name. Security is routinely bypassed by store clerks, senior executives, and anyone else who just needs to get the job done. Only when cryptography is designed with careful consideration of users' needs and then smoothly integrated, can it protect their systems, resources, and data.

THE STATE OF SECURITY

Right now, users have no good way of comparing secure systems. Computer magazines compare security products by listing their features, not by evaluating their security. Marketing literature makes claims that are just not true; a competing product that is more secure and more expensive will only fare worse in the market. People rely on the government to look out for their safety and security in areas where they lack the knowledge to make evaluations -- food packaging, aviation, medicine. But for cryptography, the U.S. government is doing just the opposite.

When an airplane crashes, there are inquiries, analyses, and reports. Information is widely disseminated, and everyone learns from the failure. You can read a complete record of airline accidents from the beginning of commercial aviation. When a bank's electronic commerce system is breached and defrauded, it's usually covered up. If it does make the newspapers, details are omitted. No one analyzes the attack; no one learns from the mistake. The bank tries to patch things in secret, hoping that the public won't lose confidence in a system that deserves no confidence. In the long run, secrecy paves the way for more serious breaches.

Laws are no substitute for engineering. The U.S. cellular phone industry has lobbied for protective laws, instead of spending the money to fix what should have been designed correctly the first time. It's no longer good enough to install security patches in response to attacks. Computer systems move too quickly; a security flaw can be described on the Internet and exploited by thousands. Today's systems must anticipate future attacks. Any comprehensive system -- whether for authenticated communications, secure data storage, or electronic commerce -- is likely to remain in use for five years or more. It must be able to withstand the future: smarter attackers, more computational power, and greater incentives to subvert a widespread system. There won't be time to upgrade them in the field.

History has taught us: never underestimate the amount of money, time, and effort someone will expend to thwart a security system. It's always better to assume the worst. Assume your adversaries are better than they are. Assume science and technology will soon be able to do things they cannot yet. Give yourself a margin for error. Give yourself more security than you need today. When the unexpected happens, you'll be glad you did.

Bruce Schneier schneier@counterpane.com <http://www.counterpane.com>

⚡ Risks in cryptography advertising (Gene Berkowitz)

"Gene Berkowitz" <geneb@ma.ultranet.com>

Sat, 09 Nov 96 23:15:38 -0500

In EE Product News (a free advertising journal for the electronics industry) October 1996, p. 13, highlighted as a "Semiconductor of the Month" was the following: (I have emphasized certain portions with *...*)

> XL103 CryptChip is claimed as the industry's first real-time encryption/
> decryption chip. *It protects data streams in applications as diverse as
> the Internet, modems, cellular telephones, pagers, and TV set-top
decoders*.

> The easy-to-use IC requires no external components and *protects data
> without the burden of learning cryptography*. Users also need not write
> complicated and difficult-to-maintain software.

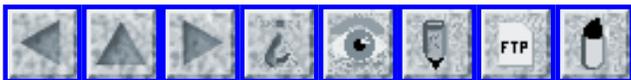
> The chip's algorithm is a protected, hard-wired circuit that's *more
secure
> than software because it can't be read or copied, preventing reverse
> engineering*.

> The chip encrypts (or decrypts) data at a rate of 6.5 bits/ms. *With the
> ability to hold eight different 64-bit keys in internal EEPROM, the device
> can handle data from eight different secure systems. In lots of 1000,
> pricing is \$0.94 each* in an 8-pin plastic DIP and \$0.97 in an SOIC.

How many RISKS are there in this single advertising blurb?

1. Assuming that one encryption method is suitable for any data type.
2. Is designed to be utilized by an engineer who has no understanding of how (or if) it works.
3. Assuming that a hardware device is more secure than a software algorithm.
4. Offering the potential attacker the ability to use 8 keys at a time for generating cyphertext and selling him the part for a buck...

--Gene S. Berkowitz



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 18: Issue 62

Weds 20 November 1996

Contents

- [Effects of the next cycle of solar interference](#)
[David L. Oppenheimer](#)
- [Lock those electronic doors](#)
[Dave Farber](#)
- [Risks of ActiveX](#)
[Simson L. Garfinkel](#)
- [New tampering attacks on smartcards and security processors](#)
[Ross Anderson](#)
- [Digital cash - just say no! Mondex/MasterCard](#)
[Nick Brown](#)
- [Computer Theft, Low-Tech Style: Visa credit information](#)
[Edupage](#)
- [The current score is: Y2K 1, Visa 0](#)
[Ry Jones](#)
- [Forwarded to X, remailed to Y, redirected to Z ...](#)
[Rob Slade](#)
- [NT password is not much protection](#)
[comments on sci.crypt item](#)
- [Large app stumbles JDK/JVM](#)
[Michael O'Donnell](#)

- [Data correct, conclusion wrong](#)
[Flint Pellett](#)
 - [Cellular One locating cell calls](#)
[Sam Lepore](#)
 - [Re: Sometimes junk e-mail is already a fax, legally speaking](#)
[Phaedrus](#)
 - [Re: AOL Bans All Mail from 53 "Junk Mail" Domains](#)
[Chris Eason](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ Effects of the next cycle of solar interference

"David L. Oppenheimer" <davido@CS.Princeton.EDU>

Tue, 19 Nov 1996 11:03:33 -0500

[Source: Coming solar cycle may pose problems, AP item, 19 Nov 1996, PGN Stark Abstracting and Excerpting Service.]

Cycle 23 of solar interference activities is building up, and is expected to have considerable effects on our planet around the year 2000, according to a panel of government researchers. (Cycle 22 was at its peak in July 1989

[see [RISKS-8.38](#), 39 on electric currents induced in power lines, blacking

out Quebec, and [RISKS-8.72](#) for a more detailed retrospective article]; the

strongest cycle to date was in November 1957.) In particular, many new

industries have emerged that were not subjected to previous solar effects --

and they have not anticipated the risks to their systems and their

businesses. Navigation and communications are considered to be particularly

vulnerable. For information on the report, you might try contacting Air

Force Col. Jud Stailey, assistant director of the Office of Federal Coordinator for Meteorological Services, a 13-agency panel housed in the offices of the National Weather Service, or Ernie Hildner, director of the National Oceanic and Atmospheric Administration's Space Environment Center in Boulder, Colo.

Potential problems to anticipate include damage to computers and other electrical systems in satellites; expansion of the Earth's atmosphere, slowing down satellites and pieces of space debris, making them harder to track; induced currents in pipelines and other large arrays of metal; disruption of signals for the inexpensive single-frequency global positioning system satellites; interference with the newly developed satellite cell-phone system; changes in the Earth's magnetic field, interfering with signals used to direct oil drilling bits deep underground.

[An obvious question for RISKS readers is which will have a more dramatic effect, Y2K or Cycle 23? Perhaps we will have Murphy-slaw and each will reinforce the other on the same day! PGN]

Lock those electronic doors

Dave Farber <farber@cis.upenn.edu>
Sun, 17 Nov 1996 20:30:15 -0500

U2-INTERNET

LONDON (AP) - The Irish rock band U2 may have become the world's first music group to be burglarized on the Internet, according to reports. Two songs lifted from the band's yet-to-be released album have been removed from computers at U2's Dublin studio and distributed on the Internet, according to the Sunday Times of London. Island Records, which manages the multi-million selling artists, says the appearance of the songs represents copyright infringement. Island is reportedly trying to close down the Internet sites on which the songs, "Discotheque" and "Wake Up Dead Man," appear.

⚡ Risks of ActiveX

"Simson L. Garfinkel" <simsong@vineyard.net>
Sat, 16 Nov 1996 13:28:40 -0500

Although people who care about computer security are concerned about ActiveX, the problems are likely to grow in the coming months and years. That's because ActiveX is key to Microsoft's long-term strategy of eliminating the distinction between information stored on desktop computers and information stored on the network.

I have had numerous conversations with Microsoft employees about ActiveX over the past six months. In summer 1996, I was told that the security problems would be solved by code-signing. This fall, I was told that code-signing doesn't solve the security problem, but does provide accountability. Now I'm told that it doesn't really give you

accountability

either, but it does give you integrity for the downloaded applets and, anyway, code signing is import for its own right. Besides, says Microsoft folks, the dangers in ActiveX controls are no different than the dangers that are found in downloading any program from the Internet.

The real reason that code signing does not promote authentication, of course, is that truly malicious ActiveX components won't tell you that they are maliciously modifying your operating system. In fact, they'll try to make the modifications as quietly as possible. Or they might engage in a two-pronged attack. For example, one ActiveX control could change Internet Explorer's ActiveX security level so that you would run unsigned applets; later, a second control could do the real damage.

On Wednesday, November 20th, my column on HotWired's "Packet" channel will go into the ActiveX security problem in some detail. If you wish to read it, just check out <http://www.packet.com/garfinkel>. It's free.

Simson Garfinkel

✦ New tampering attacks on smartcards and security processors

Ross Anderson <Ross.Anderson@cl.cam.ac.uk>

Sat, 16 Nov 1996 18:46:41 +0000

A number of posts on breaking tamper resistant processors have appeared recently; most of them have been theoretical. However, in a

paper to be published on Tuesday, we describe a number of very practical attacks on smart cards and other security processors. We have implemented some of them successfully against fielded systems.

The URLs are:

html: www.cl.cam.ac.uk/users/rja14/tamper.html
postscript ftp.cl.cam.ac.uk/users/rja14/tamper.ps.gz

This work will appear at the Usenix Electronic Commerce workshop in Oakland, California, where it has won the 'Best paper' award. It was written some time ago, but we held back the results in order to give banking systems developers the chance to implement countermeasures.

One of the attacks we describe breaks completely a security processor that is widely used in the banking industry; it is embedded in about a million point-of-sale terminals, automatic-teller machines, and banking key management systems. Our attack enables all the code and key material to be read out from this chip in minutes.

Other techniques we describe enable attackers to extract all or part of the code and keys from various makes of smartcard and 'secure' microcontroller. They have profound implications for bankers, pay-TV stations, operators of prepayment electricity meters and of course for the smartcard industry itself.

We also include a survey of attacks developed by others, many of which have not appeared in the literature before. We found that once we had some

results to show, everyone from chipmakers through intelligence agencies to TV pirates wanted to swap hints and compare notes. Even some top scientists at smartcard companies would tell us about vulnerabilities - in their competitors' cards!

So our article describes a number of the attacks actually used by spooks and TV pirates. We also describe techniques developed by the chip testing industry, many of which can easily be adapted to read out secrets from smartcards; although they are in the open literature, the security community has just not been aware of them.

Until quite recently, many system developers relied blindly on the tamper resistance claims made by the manufacturers of smartcards and other security processors. Over the last two or three years, it has become increasingly clear that organised gangs had acquired the capability to clone the smartcards used in pay-TV access control. This raises the obvious risk that banking systems could be next.

Since writing this paper, we have devised a number of additional attacks.

For example, Biham and Shamir announced an attack on DES based on 200 ciphertexts in which one-bit errors have been induced by ionising radiation; we can break DES with less than ten ciphertexts, using the kind of faults introduced by power and clock glitches. Boneh, DeMillo and Lipton announced an attack on RSA using one-bit errors; we can break RSA with a one-round glitch attack. This could be implemented in a Mafia-owned point

of sale
device, and factor RSA moduli in real time without the attack
being noticed
by either the customer or her bank.

Our techniques not only make Differential Fault Analysis much
more
efficient; the fault model that we use is completely realistic.
No-one has
to our knowledge implemented an attack using radiation to
generate one-bit
data errors, but using high frequency transients in the power
and clock
inputs to a smartcard is an established way of causing it to
decode
instructions incorrectly. This technique has actually been used
by TV
pirates - though they attacked the card protocols rather than the
cryptographic algorithms.

Once we can cause instructions to be wrongly decoded, a range of
quite novel
attacks becomes available. In addition to differential fault
analysis, we
can look for glitches that reduce the number of rounds in the
encryption
algorithm. If DES is reduced to one or two rounds, for example,
then
extracting the key becomes trivial.

This attack can also be implemented using our most recent
innovation - the
ROM overwrite attack. This is inspired by the observation that
many
smartcards have a DES implementation in ROM, which we can
usually see under
a microscope and which we can damage using a laser cutter. This
is often a
lot cheaper and simpler than using an ion beam workstation to
read keys
directly out of EEPROM.

If we are familiar with the ROM implementation (or can

disassemble

it), we typically find a small number of bits with the property that changing them reduces the number of rounds to one or two. Where this is not possible, we may still be able to identify the S-boxes, and by setting all their bits to the same value we can turn DES into a linear transformation. Again, the key can be trivially recovered.

This is a new and exciting field of research, and one that secure system designers would be prudent to follow closely.

Ross J. Anderson
Computer Laboratory
University of Cambridge
Pembroke Street, Cambridge CB2 3QG
E-mail: ross.anderson@cl.cam.ac.uk

Markus G. Kuhn
Department of Computer Sciences
Purdue University
West Lafayette, IN 47907
E-mail: kuhn@cs.purdue.edu

✶ Digital cash - just say no! Mondex/MasterCard

+33)388412674 <"Nick Brown" <Nick.BROWN@DCT.coe.fr> (Tel>
19 Nov 1996 15:42:01 +0000

Apparently MasterCard has bought a 51% share in Mondex, a British company which produces electronic cash smart cards. Mondex has been on pilot tests in Swindon, England, for the past year or so, and MasterCard claims to want to make it available across Britain.

Am I the only person who thinks this is suicidal, either for MasterCard and its associated banks, or in the worst case for the whole currency?

The arrogance of the people behind this and other forms of virtual money, in thinking that their codes can't be defeated by either brute-force or backdoor mechanisms, is quite breathtaking. [RISKS-18.15](#) has an example of how this kind of thing has already been done. And when the Mondex trial system was launched, BBC Television showed how easy it is to retrieve all kinds of smart card technical data over the Internet.

Once those smart cards, readers, and ATM card-point-loaders get widely distributed, they will be sitting targets for anyone who fancies a shot at reverse-engineering them. Possible reward: a machine that effectively prints money, but far, far more attractive than forging bills. I think the bad guys might have a few 200 MHz Pentium Pro systems to spare for this; although in any case, stealing just one card-loading machine would seem to be simpler.

For one thing, a fake bill is still a fake bill after it's been passed on ten or a hundred times, and the person introducing it into the system knows that, for the first few times each bill is used, there's at least some possibility of tracing it back. For fake electronic cash, however, there's no way to distinguish between the real virtual stuff and the fake virtual stuff. As a result, nobody will care whether what they're being given is

real or not, like they currently do with those fancy U-V lights, because they won't have it rejected by the bank.

Having any ATM able to load up your smart card with points, is equivalent to having current ATMs print the bills fresh 'n' crisp when you ask for them, and just making a mental note to settle up with the central bank later. For a number of very good reasons, central banks don't like the idea of this. (Does anyone imagine that the directors of BCCI would have bother ripping off their customers, had it been easier just to print a few bills and forget to notify the Federal Reserve or Bank of England ?)

Even worse, the only way we'll know that there are a lot of fake Mondex cash in circulation is when inflation starts rising for no obvious reason; at which time, the crisis in confidence in the banking system doesn't bear thinking about.

One other point that I am reluctant to make, since I don't usually subscribe to the "drug dealers/paedophiles/foreign agents use technology item X, so we have to make it illegal, to protect our streets/kids/national security" argument, but: has anyone considered just what a great tool this will be for laundering money ?

Nick Brown, Strasbourg, France

🔥 Computer Theft, Low-Tech Style: Visa credit information

Edupage Editors <educom@elanor.oit.unc.edu>

Tue, 19 Nov 1996 23:06:40 -0500 (EST)

A thief broke into a Visa International data processing center in California a couple of weeks ago and stole a personal computer containing information on about 314,000 credit card accounts, including Visa, MasterCard, American Express, Discover and Diners Club, says a Visa spokesman. Some issuers, including Citibank, began calling customers last week and have issued new cards. Others are keeping quiet about the event and monitoring accounts for unusual activity. Authorities speculate that the perpetrator was stolen for the resale value of the hardware, rather than the information it contained.

(*St. Petersburg Times*, 19 Nov 1996 E2)

⚡ The current score is: Y2K 1, Visa 0

Ry Jones <rjones@halcyon.com>

Mon, 18 Nov 1996 11:49:08 -0800 (PST)

<http://www.msnbc.com/news/42003.asp> discusses the ramifications of the embedded technology in card swipe readers not being Y2K compliant. The article states that 10% of the Visa swipe readers cannot deal with Y2K expiration dates, marking the cards as invalid because 1900 < the current day/time. Visa cards are issued with 3 year expiry periods, meaning the first batch of reader-breaking cards is probably already in consumer hands.

The article also states that Visa will levy fines on member banks from 1000 USD to 100000 USD for non-compliance with a directive to fix all merchant systems by March 1997.

In the interim, Visa is asking member banks not to issue cards that expire in Y2K, instead, issuing cards that expire in 1999. My favorite quote from the web page: "(It seems that using two-digits rather than four to represent a year was once a common programming technique)".

🔥 Forwarded to X, remailed to Y, redirected to Z ...

"Rob Slade" <roberts@mukluk.hq.decus.ca>
Mon, 18 Nov 1996 14:21:08 EST

I suppose there is nothing much new in mailstorms, or in the problems of forwarders and remailers, but ...

As some RISKS readers may be aware, I occasionally submit reviews of books to the list. In fact, this is only a small selection from the book reviews that I "publish" daily over the net. I do not run an automated mailing list myself, submitting the reviews for the general public via the Usenet *.books.* groups. I do manually maintain a select mailing list for newsletter publishers, bookstores, and Web site archivists.

A little over a week ago I started to get a flurry of bounce messages from one site. In fact, I was getting around a hundred messages per day. In addition, for some reason the messages were of extraordinary

size, and were regularly causing my account (on a VMS system) to exceed disk quota.

Often this type of thing is caused by the remailing of one of my messages through another mailing list. NETTRAIN (for perhaps obvious reasons) seems to have a very high proportion of people who simply abandon their accounts without unsubscribing, and these accounts frequently bounce errors to the originator, rather than the list-owner. Examination of the header, however, showed no indication that this had happened in this instance. My own list had no entry that remotely resembled the site I was getting the bounces from.

This has gone on for the past week. All the bounces relate to the one, single message: none to any subsequent reviews sent out. Messages to every "postmaster" account I could generate from the header info turned up nothing.

The bounces haven't stopped, but I've finally got some information on whose account it is. One of the requests to be put on the list was for a small, local distribution list. One of the people on that list does not work directly for the people running the local list. She was provided with an account on their system, but never learned to use it. Her lack of use of the local account created a problem with mail buildup on their local system, so that account was forwarded to her work.

Her work system seems to be the one generating the problem.

Apparently they have had unresolved network connection problems for some time now. It seems reasonable to assume that something tried on that one day has now created an unresolved loop, which is still sending out the error messages.

My problem still isn't resolved. Of course I have now taken the system with the local distribution off *my* list, thus ensuring that no more mail goes to them, her, or her employers. In the meantime, the bug has taken on a life of its own, plugging my e-mail account (and exceeding my quota) on a daily basis.

Isn't automation wonderful? :-)

roberts@decus.ca rslade@vcn.bc.ca slade@freenet.victoria.bc.ca
link to virus, book info at <http://www.freenet.victoria.bc.ca/techrev/rms.html>

⚡ NT password is not much protection (comments on sci.crypt item)

RISKS List Owner <risiko@csl.sri.com>

Tue, 19 Nov 96 9:59:55 PST

[Identity of contributor withheld by request.]

Recently, sci.crypt, Bernd Lehle wrote:

- > On <http://www.omna.com/Yes/MWC/PRS-index.htm> a company called MWC offers
- > the following service:
- >
- > "recover" an NT (any version) Administrator password at any

level of
> complexity within 4 hours.
>
> They claim to use 4 PPro-200s and guarantee the result for a
fee of
> US\$4500.
>
> NT uses up to 14 characters in a password. In order to recover
a UNIX
> password at any level of complexity with 14 characters, 4 PPro-
200s will
> crunch for approx. 1e16 years (assuming 10,000 crypts per CPU
per second).
> Does anybody know, where the difference comes from ?

Jeremy Allison <jra@cygnus.com> replied:

> Yes, this is very interesting. I believe I know
> how they are doing this. They have discovered a
> nasty little 'secret' in NT that I have been pursuing
> for a couple of years now (on and off, without really
> dedicating months of time to it though :-).
>
> My guess would be, if you sent them a drive and
> told them you had lost your password, it would come
> back with a different Administrator password than
> the one you sent it in with :-).
>
> It works like this. The NT password database in the
> registry is only as secure as UNIX shadow passwords
> (actually, a little less secure as they don't use
> salt in their hash technique, it's pure DES for the
> Lanman password, and MD4 for the NT password).
> The 'nasty little secret' is that the hashed password
> values are double encrypted (for 'obfuscation purposes'
> it says in the NT knowledgebase) in the SAM. I believe this
> company has worked out how that double encryption is done,
> and just overwrite the hashed password. My explorations in
> this area lead me to believe that MS use DES in ecb mode
> to just encrypt the hash, and that the key is some
> function of the last RID component of the users SID value.
>
> I believe this to be the case after doing various
> experiments on an NT SAM database, changing users

> names whilst keeping password the same (no change
> in double-encrypted hash), assigning the same password
> to users with the same name but different SID's (different
> double encrypted hash), assigning the same password to
> users with different names, in different domains, but
> with the same last RID component of the SID (identical
> double-encrypted hash). ...

[With minor spelling corrections. PGN]

⚡ Large app stumbles JDK/JVM

Donkey Hotay <mod@world.std.com>

Wed, 13 Nov 1996 12:33:32 -0500

The article at <http://www.techweb.com/wire/news/1109bug.html>
describes

how "A prominent Web development shop found two substantial
performance
flaws in Sun Microsystems' Java Developers Kit when it attempted
to
deploy it in a large-scale environment." The developers'
introduction
to various RISKS will be familiar to readers here. Excerpted
comments:

"In a complex, multiserver, multiprocess environment, that's to
be
expected," Presence's McFall said. "We had to tune several
things
before we could get it stable." Once the AtHand design was
stable,
the problems in the Virtual Machine emerged. As the load
increased
between the Web server and an Oracle database on the AtHand
site,
the Virtual Machine locked up.

"Some of the operations, as far as managing memory, worked under

normal load, low-stress conditions, but when you start pounding on it--like what is going to happen on a big Web site--there are a few bugs in there," said Xeno Derer, the software engineer at Presence charged with fixing the Java bugs. "It either died thinking it was out of memory or the Virtual Machine itself would start crashing."

The article mentions that PacBell was the client and that the app was to handle, among other things, their online directory service.

Michael O'Donnell mod@std.com

✦ Data correct, conclusion wrong (Re: Baker, [RISKS-18.58](#))

Flint Pellett <flint@kai.com>

Fri, 15 Nov 1996 17:19:57 CST

> "However, the market was not kind to Symbolics, proving that software quality is not a particularly important feature in a computer system, as judged by paying customers."

Mr. Baker's conclusion does not seem warranted based on the evidence he presents. Paying customers make their buying decisions based upon a lot of different factors such as cost, performance and features. Quality is certainly one of them.

Mr. Baker is welcome to release a really low-quality software product out into the marketplace to prove me wrong. If he is right,

he'll be
rich a year from now.

✦ Cellular One locating cell calls (Re: Glassman, [RISKS-18.40](#))

<Sam.Lepore@ncal.kaiperm.org>

Tue, 12 Nov 1996 06:05 -0800 (PST)

In early September, Bernard Glassman wrote about FedEx using a service provided by Cellular One in North Carolina to locate the point from which he originated a cell call.

I pursued the question about that service availability with my local (San Francisco Bay Area) Cellular One office. They responded in writing:

"Cellular One Bay Area does not offer the service described in the e-mail.

It is important to remember that Cellular One is a franchise and each

service area is individually owned and operated. I will of course contact

you if I hear of any such services being offered by our company."

It seems there is a risk of assumption in dealing with a company that appears to be a national entity but is in fact a series of franchises. We should not assume all locations will deliver (or not deliver) the same services.

I can't recall ever having heard that different locations of any company might offer different services _because_ the company is a franchise ...

unless it is the ubiquitous phrase on hamburger advertisements
"at
participating locations only" ?

Sam Lepore Kaiser Permanente Walnut Creek, California

✉ Re: Sometimes junk e-mail is already a fax, legally speaking

Phaedrus <phaedrus@halcyon.com>

Sat, 14 Sep 1996 09:46:27 -0700

If you accept that 47 USC 227 does apply to e-mail, let me point out that Mr. Franklin has violated that same federal law by sending his message to comp.risks, and our esteemed moderator has also violated the law by distributing RISKS. This is because that law also contains the following clause:

"It shall be unlawful for any person within the United States [...] to use a computer or other electronic device to send any message via a telephone facsimile machine unless such person clearly marks, in a margin at the top or bottom of each transmitted page of the message or on the first page of the transmission, the date and time it is sent and an identification of the business, other entity, or individual sending the message and the telephone number of the sending machine or of such business, other entity, or individual."

In other words, if you believe that 47 USC 227 applies to e-mail, and you have ever sent an e-mail message that did not include your

telephone number,
then you are a federal criminal. (And there's still the thorny
issue of
deciding exactly what constitutes a "page" of an e-mail message.)
Furthermore, the manufacturer of your computer has violated the
law, because
the law also requires the manufacturers of telephone facsimile
machines
after 1992 to make sure that the machine clearly marks this
information on
each page.

There are several other aspects of 47 USC 227 that make no sense
in this
context. I would certainly agree that a law against unsolicited
bulk e-mail
is called for. But the way to solve that problem is to create
such a law,
not to try to creatively misconstrue an existing law to cover a
situation it
wasn't designed or intended for.

⚡ Re: AOL Bans All Mail from 53 "Junk Mail" Domains

<ChrisEason@aol.com>

Fri, 8 Nov 1996 21:57:33 -0500

As an AOL subscriber, I would like to clarify this situation.
AOL did not ban
these domains, they simply provided their users with the tools
to block mail
from them. Any AOL subscriber can receive mail from any or all
of the domains
by setting the appropriate flags.

The risk here is that AOL's member accounts are automatically
set to block
these domains, and it's up to the individual members to know
that they need

to unblock them if they want to receive the mail. AOL did advertise this option conspicuously on the service.

Chris Eason



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 18: Issue 63

Tuesday 26 November 1996

Contents

- [Mars Probe crashes](#)
[Ben Morphet](#)
- [Massive NY tax fraud](#)
[Mich Kabay](#)
- [Complexity of the airplane pilot's interface](#)
[Mich Kabay](#)
- [Bell Atlantic 411 outage](#)
[Rich Mintz](#)
- [DIMACS Network Threats workshop, Rutgers, 4-6 December 1996](#)
[Rebecca Wright](#)
- [Year 2000 Problem Will Cause Lawsuits, Bankruptcies](#)
[Edupage](#)
- [Y2K *Guardian* article on retroactive liability](#)
[Martin Minow](#)
- [Danish government puts its own records on the Web, illegally](#)
[Ketil Perstrup](#)
- [Badly placed hardware](#)
[Abigail](#)
- [Digital footprints on the Internet](#)
[Martin Minow](#)

- ["Disappearing Cryptography" by Peter Wayner](#)
[Rob Slade](#)
[Peter Wayner](#)
 - [Re: Effects of the next cycle of solar interference](#)
[McInnis](#)
 - [Risks of believing what you read: Re: Irish rock band](#)
[Stuart Woodward](#)
 - [The SEI Conference on Risk Management](#)
[Carol Biesecker](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✂ Mars Probe crashes

Ben Morphett <ben@jna.com.au>
Thu, 21 Nov 1996 09:28:23 +1100 (EST)

When the Russian Mars probe crashed earlier this week, it provided an interesting example of the difference between precision and accuracy.

The first reports said that the probe would crash land in central Australia, bringing with it 200 g of plutonium. State emergency services all over Australia went into yellow alert. Soldiers were mobilised.

>From the TV pictures, the first estimates of where it would land were anywhere in an area about 2000 km across. The next reports said that it would be landing at about the New South Wales/Queensland border, and they seemed to think it would come down somewhere in an area about 500 km across. The next reports said that it would come down somewhere in an area in the north west of New South Wales, and the precision of this estimate seemed to

be about 100 km.

As it turned out, it came down about 2000 km west of Chile, in the Pacific Ocean, a third of the way around the world from Australia.

So as the precision of the reports was increasing, the accuracy of the reports was about staying about the same - very wrong.

Ben Morphett ben@jna.com.au

✶ Massive NY tax fraud

Mich Kabay <75300.3232@CompuServe.COM>
22 Nov 96 12:36:43 EST

Hacker Scheme, By KAREN MATTHEWS, Associated Press Writer
NEW YORK (AP) -- City workers, in exchange for bribes from property owners, falsified computer records to eliminate nearly \$13 million in unpaid taxes in a scheme called the largest tax fraud case in New York City history. [Associated Press news wire via CompuServe's Executive News Service, AP US & World, 22 Nov 1996]

The author makes the following key points:

- o Some tax records erased.
- o Other records falsely indicated as paid using funds from legitimate payments by innocent victims.
- o So far, 29 people charged in federal court.
- o 200 more expected to be charged.
- o \$13M of debts erased.
- o \$7M in interest lost.
- o Fraud thought to have started in 1992.
- o Investigation started in 1994.

- o In a section particularly intriguing for RISKS and NCSA FORUM participants,
the author writes, ``Three employees of the city collector's offices exploited computer "glitches" to make it appear that unpaid taxes had been paid, officials said.

More, no doubt, as the case unfolds.

M. E. Kabay, Ph.D. (Kirkland, QC), Director of Education
National Computer Security Association (<http://www.ncsa.com>)

✶ Complexity of the airplane pilot's interface

Mich Kabay <75300.3232@CompuServe.COM>
25 Nov 96 16:06:50 EST

This item from last week in Executive News Service on CompuServe caught my eye:

Pilots said stretched to limit by cockpit high-tech
Reuters World Report, 20 Nov 1996

LONDON, Nov 20 (Reuter) - Airline pilots are being stretched to the limit by increasingly complex cockpit technology and need radically different training methods to cope in future, a top medical aviation specialist said on Wednesday.

The article makes the following key points:

- o Dr Michael Bagshaw is head of aviation medical services at British Airways. He wonders, "Are we perhaps reaching the limit to pilots' mental processing capacity?"
- o However, he answered in his address in London to the Royal Society in London, "On the face of it we may have reached a plateau. But experience shows that having reached a

plateau,

we then move on again."

- o According to the expert, "In both military and commercial aviation the complexity of the environment is increasing. Automation is being developed but the question remains as to whether the automation relieves workload or increases it."
- o "If we examine the accident rate by type of aircraft, it can be seen that although the overall trend is down ... new highly-automated types have a relatively higher accident rate."
- o In some cases, plane design prevents manual overrides even if the automated system is in trouble.
- o The increasing use of CRT and LCD displays means that what used to be on separate dials now appears, in the words of the author of the article, "on one cluttered computer display, which meant pilots needed to spend more time interpreting what they were seeing."
- o Dr Bagshaw added, "We are starting to see some of the limitations of information processing. This is the weak link -- information is derived from a number of sources. It has to be integrated, then interpreted, and the appropriate action taken to use that information appropriately."
- o The changes in technology necessitate new methods of training:
"I think we can move on from the plateau by altering the way we approach training. We've now reached a watershed by accepting that human error is normal," said Bagshaw after his speech. "The old approach was to think that human error was a mistake which should be avoided. Now we have to assume it will happen and instead assess how pilots cope with error."

M. E. Kabay, Ph.D. / Director of Education

⚡ Bell Atlantic 411 outage

Rich Mintz <mintz@netresponse.com>

Tue, 26 Nov 1996 11:18:10 -0500

On Monday 25 Nov 1996, Bell Atlantic -- the local telephone company serving the mid-Atlantic region of the USA, including Philadelphia and Washington, D.C. -- saw an outage of several hours in its telephone directory assistance service, due (apparently) to an errant operating system upgrade on a database server. For unknown reasons, the backup system also failed. The result was that for several hours, telephone operators ended up taking callers' requests and telephone numbers, looking the requested information up in printed directories, and calling the callers back with the information.

Apparently, the problem was solved by backing out the software upgrade. Significantly (in my opinion), the Washington Post's article on the outage mentioned this fact (albeit in slightly less technical language), which is yet another indication of the pervasiveness of software, and of the growing number of people in society at large that are generally aware of software and how it works.

⚡ DIMACS Network Threats workshop, Rutgers, 4-6 December 1996

Rebecca Wright <rwright@research.att.com>

Mon, 25 Nov 1996 14:57:02 -0500 (EST)

DIMACS Workshop on Network Threats

Sponsored by the DIMACS as part of the 1996-97 Special Year on Networks

December 4-6, 1996

DIMACS Center, CoRE Building (Computer Research and Education)
Rutgers University Busch Campus
New Brunswick, New Jersey, USA

Workshop organizers:

Steve Bellovin, AT&T Labs - Research, smb@research.att.com

Peter G. Neumann, SRI International, neumann@csl.sri.com

Rebecca Wright, AT&T Labs - Research, rwright@research.att.com

As the use of computer networks, and in particular the Internet, has increased, so has the potential threat to security. In the last several years, we have seen numerous security-related attacks on Netscape, Java, and the Internet protocols. New protocols and systems for electronic commerce, secure financial transactions, and other applications are being introduced, and are being deployed quickly, and on a large scale. This workshop aims to bring together theorists and practitioners working in areas related to network security in an informal setting to foster discussion regarding the nature of the threat and what we, as researchers, can do to help manage it.

Confirmed speakers:

Steven M. Bellovin (AT&T Labs - Research)
Bill Cheswick (Bell Labs)
Shiu-Kai Chin (Syracuse University)
Cindy Cullen (Bellcore)
Drew Dean (Princeton University)
Yvo Desmedt (University of Wisconsin - Milwaukee)
Ed Felten (Princeton University)
Robert J. Hall (AT&T Labs - Research)
Catherine Meadows (Naval Research Laboratory)
Peter G. Neumann (SRI International)
Sarvar Patel (Bellcore)
Jean-Jacques Quisquater (Universite de Louvain)
Alexis Rosen (PANIX Public Access Networks Corporation)
Avi Rubin (Bellcore)
Adam Shostack (Consultant)

There is still room in the schedule for a few more talks. If you would like to give a talk describing current, unpublished work, please

e-mail a 1-2 page abstract (postscript or plain ASCII text) to Rebecca

Wright at rwright@research.att.com.

MORE INFORMATION:

The full workshop program, plus information regarding registration, travel and local arrangements for this workshop can be found at:

<http://dimacs.rutgers.edu/Workshops/Threats/index.html>

⚡ Year 2000 Problem Will Cause Lawsuits, Bankruptcies

Edupage Editors <educom@elanor.oit.unc.edu>

Sun, 24 Nov 1996 15:12:08 -0500 (EST)

At a recent meeting sponsored by the Electronic Banking Economics Society,

one speaker predicted that a bankruptcy rate of between 1% and 5% could result directly from costs related to fixing the notorious "Year 2000 Problem." "If you have not yet begun a Year 2000 conversion today, you will not be able to convert by 2000," he said, noting that there are only 150 weekends left to work on systems affected by the problem. If companies choose to ignore the problem, they'll be liable for millions in lawsuits brought by shareholders when company stock prices begin to plummet. Only one third of U.S. companies are addressing the problem, with another third entering the preliminary discussion phase, and the other third doing nothing. Still, that's better than the rest of the world: "Britain is three steps behind the United States on this issue, Europe about 10 steps behind the United States on the issue, and Japan is about 15 steps behind the United States on the issue," the consultant said. (*BNA Daily Report for Executives*, 20 Nov 1996, A16; Edupage, 24 Nov 1996)

✶ Y2K *Guardian* article on retroactive liability

Martin Minow <minow@apple.com>
Thu, 21 Nov 1996 16:26:33 -0800

The online edition of the Guardian newspaper has an interesting article on the year 2000 problem; concentrating on the legal responsibility of software and hardware vendors.

The article quotes Stephen Castell, a consultant in computer

technology:

"Castell believes that around the beginning of 1992 is the earliest time from which suppliers may be liable. He says, "The problem was sufficiently recognised in the industry from around then, and systems developers should have considered moving on from the two-figure date." However, if it is correct that the potential problem should have been obvious, courts may be less indulgent to developers who overlooked it even before 1992."

<http://go2.guardian.co.uk/computing/961121coonUpagainstthecloc.html>

(Note that the Guardian may only archive articles for a short time.)

Martin Minow minow@apple.com

🚩 Danish government puts its own records on the Web, illegally

Ketil Perstrup <ketil@diku.dk>

Fri, 22 Nov 1996 15:28:58 +0100

Many of the requests processed by local government offices are requests for information from government records. This fact has given the Danish Ministry of Research a seemingly brilliant idea: Making government records available on the World Wide Web would free local government officials from processing these requests.

The first government records were made public on October 1 on <<http://ditdanmark.nethotel.dk/vurdering/>>. The information was taken from the land and building property evaluation records of the Danish

Tax
Ministry. These records are used by employees in the tax offices
of the
local government for taxation of land and building property. The
published
information included the following for each piece of land and
building
property in Denmark: Location, owner, estimated value, date and
price
(including down payment) of last sale (if sold since last
evaluation of the
property in 1992), debts to local government, rental value for
non-residential property (if rented) and further notes intended
to assist
evaluation.

On the October 15 the records were made inaccessible when the
large,
reputable Danish newspaper Berlingske Tidende published a
critique by
professor Erik Frøkjær from the Department of Computer Science at
Copenhagen University. Two things were criticized:

1. The records could be copied without explicit permit by anyone
with
access to the Internet, something which is not allowed according
to the
Danish Public Authorities' Registers Act.

2. The last three items in the list above were confidential
information and
could not legally be published under Danish law.

Access to the records was reestablished the next day when the
offending
items had been removed. At that time the publisher, Kommunedata,
assured
the public and the Danish Data Surveillance Authority
("Registertilsynet")
that the records could not be copied. The company also publicly
explained
that Erik Frøkjær could not possibly have copied the records
except by

means that were not entirely legal.

Soon after this a group of researchers contacted the Danish Data Surveillance Authority to demonstrate that the records are easily copied (with entirely legal means), but the offer of a demonstration has been declined by the Authority. Copies of the case obtained from the Authority under the Danish Freedom of Information Act show that the Authority has been made aware by other means that copying is possible. Despite this the Authority refuses to take action based on this evidence so WWW access is still possible. The only change since the reopening has been removal of most of the information about sales when the Court in Århus informed the Authority that this information is not and should not be publicly available.

This is the first case known to me of government records being published on the World Wide Web. The case is instructive: There has been repeated valid objections to the legal basis on which the records are made available. This and the fact that the continuing operation of this service is not important for anything but the reputation of the parties involved, leads me to expect that access ought to be at least temporarily suspended until the questions were resolved.

This case demonstrates a large collection of security problems inherent to World Wide Web publication of government records as well as a lot of legal problems that will not be mentioned here. These problems are probably compounded because both the Danish government and Kommunedata

wants to be
perceived as technologically advanced and "Internet-friendly".

1) The original records were used by the employees in local tax offices, so information that was not meant to be disclosed publicly was maintained together with the evaluation of each piece of property. When the records were made available on the World Wide Web without cleanup, confidential information was disclosed. Moral: When sensitive information is put to use in a new way it should be checked to make sure that all information is appropriate for the new use.

2) The Danish Data Surveillance Authority does not have its own technical staff, so it wasn't able to assess the correctness of the claim made by the publisher, Kommunedata, that the records could not be copied. Moral: Government authorities should not rely on experts employed by the companies that are checked. When new types of problems are encountered the government should use their own or independent security experts to assess the claims made by companies.

3) It is not possible to prevent information published on the Internet from being copied, so information that must not be copied should not be available on the Internet.

4) Until now the companies and government authorities involved has ignored criticism from computer professionals. Moral: Government officials does not automatically listen when professionals criticize security. If the critique

goes against official policy you might very well be ignored or worse, no matter how serious the problem is.

5) Denmark prides itself on its large information systems in the public administration. These information systems have been accepted by the public because of a set of very restrictive laws governing these records and strict attention to security. Other governments may be tempted to publish similar records on the World Wide Web because when the security-conscious Danes do it, it must be OK.

6) To add insult to injury the programs used by Kommunedata to control access to the records performs no parameter validation which shows that this publication probably has yet more security problems in store.

Despite the problems with publication of the records the Ministry of Research and Kommunedata wants to make even more sensitive and personal data available on the World Wide Web in the future. I shudder as I contemplate the consequences.

Ketil Perstrup (ketil@diku.dk)

⚡ Badly placed hardware

"Abigail" <abigail@ny.fnx.com>
Thu, 21 Nov 1996 01:52:04 -0500 (EST)

Two days ago, I was in a computer room of a large financial institution. A

whole range of different computers is in that room. One (PC) setup consisted of a tower on the ground, and a monitor and keyboard on a table. Nothing usual here. But the monitor was placed on a box which had switches for the monitor, the tower, and a printer, and a masterswitch, on one end, and cables on the other. The switches where facing forward.

The machine was happily minding its own - important - business.

My partner and I were working on a different machine. At one moment, he gives way to let me handle the machine. He puts his elbow on the table, slightly disturbing the keyboard, which is moved enough to just have the master switch break the contact for a moment, causing the machine to crash.

- "Is that serious?", he asked.
- "It is a live machine..."

When I left two hours later, at least 5 people had been trying to get it working again, and at least 10 nervous people asked what was going on. They were still trying to boot it.

Today I was in the room again. They had turned the box 90 degrees.

Abigail

🔥 Digital footprints on the Internet (Article in UK Guardian)

Martin Minow <minow@apple.com>

Thu, 21 Nov 1996 12:21:15 -0800

The online edition of the UK Guardian newspaper has a long article on the way that "Internet users leave traces and records of every online action, from sending e-mail or posting to newsgroups to visiting Web sites."

... At the moment unwanted e-mail is about the limit of the intrusion, but

this could change. Internet commentator Dominique Paul Noth points out:

"You have no guarantee that the information is intelligently or even accurately employed to your benefit." As more information is collected, it is more useful to those collecting it - and less easily controlled.

... One alternative is making yourself anonymous by deleting cookie files and using mail programs that disguise your identity.

However, making yourself anonymous online means that you cannot personalise Web pages, ask for information via e-mail, or join mailing

lists. The issue, as Noth and other commentators recognise, is more to do

with how this information is used. Credit card companies know what we are

buying, and there is a legal framework to control their use of this

information. There is no such framework in force for online information.

It seems that the very lack of "real world" controls over online activity

which many Internet users favour has created the environment in which

marketing companies can thrive. As long as the Internet is seen as somehow

outside the reach of the law, then there will be those who abuse its

freedom. So as you surf for Christmas presents, look out for

surprises in
your mailbox as a result.

The full article is at
<http://go2.guardian.co.uk/internet/961121wwonDigitlafootprint.html>

(However, note that newspaper articles on the Web are often only visible for a short time.)

Martin Minow minow@apple.com

✶ "Disappearing Cryptography" by Peter Wayner

"Rob Slade" <roberts@mukluk.hq.decus.ca>

Mon, 25 Nov 1996 11:15:46 EST

BKDSRPT.RVW 960902

"Disappearing Cryptography", Peter Wayner, 1996, 0-12-738671-8, U
\$29.95

%A Peter Wayner pcw@access.digex.net

%C 1300 Boylston Street, Chestnut Hill, MA 02167

%D 1996

%G 0-12-738671-8

%I Academic Press Professional

%O U\$29.95 +1-617-232-0500 +1-800-3131277 app@acad.com

%P 295

%T "Disappearing Cryptography"

The title seems to allude to, and the book jacket definitely trumpets, steganography, the act or art of "hiding in plain sight". An example of a steganographic message would be one which appears to be an innocuous and ordinary family letter, but which carries detailed information in the background. One chapter of the book does deal with this type of encryption,

although only in terms of hiding text data in pictures. The book as a whole seems more like a collection of essays on topics related to encryption.

The topics represented cover a broad range of information science. The level of detail provided varies, but in general the explanations are fairly simple.

copyright Robert M. Slade, 1996 BKDSCRIPT.RVW 960902
Vancouver Institute for Research into User Security Vancouver
Canada V7K 2G6
ROBERTS@decus.ca rslade@vanisl.decus.ca Rob.Slade@f733.n153.z1.fidonet.org

✶ "Disappearing Cryptography" by Peter Wayner

Peter Wayner <pcw@access.digex.net>

Tue, 26 Nov 1996 09:43:08 -0500

Rob Slade is right. Much of my book, *_Disappearing Cryptography_* is filled with simple discussion. It was intended to offer many casual readers some insight into how morphable information can be. This is a highly important technical topic these days because of the battles over encryption regulation. Sure, I could have written a nerd opera, but that wouldn't have helped people without an advanced degree in number theory. This topic is so important for policy that I wanted to try and spread the knowledge around a bit.

I think he's wrong on other counts. The book discusses how to use error-correcting codes, encryption, dining cryptographers

networks,
compression functions, and compiler technology to make
information look like
something else. I think that each of these solutions offers a
unique way to
make information `disappear' because, if it looks like something
innocuous,
then it escapes detection.

My home page (<http://www.access.digex.net/~pcw/pcwpage.html>) has
the table
of contents for those that are interested. Feel free to write
if you have
more questions. [A minireview by your moderator is in [RISKS-
18.17](#). PGN]

✉ **Re: Effects of the next cycle of solar interference ([RISKS-18.62](#))**

McInnis <mcinnis@austin.ibm.com>
Thu, 21 Nov 1996 10:52:43 -0600 (CST)

I guess one's man's poison is another man's feast.

I got a kick out of the article about the problems that could be
caused by
the next peak of the 11-year sunspot cycle. Most of us amateur
radio
operators are waiting in breathless anticipation for the
sunspots to pick up
because it "turns on" some of the radio frequencies to long range
communications. It's sort of like a starry-eyed 4 year old kid
waiting for
Christmas hearing someone grumbling about how they don't like
Christmas.

Also, the 11-year sunspot cycle has been going on for several
hundred years
since the last gap in the cycle. It says something about our
technology

that some systems might not be prepared for it. It's like someone being surprised that it's getting cold as winter approaches. ("Gee, didn't it start getting cold about this time last year, too?")

73 de KB5YAC Mickey McInnis - mcinnis@austin.ibm.com

⚡ Risks of believing what you read: Re: Irish rock band ([RISKS-18.62](#))

Stuart Woodward <stuart@gol.com>

Fri, 22 Nov 1996 17:13:18 GMT

> ... first group to be burglarized on the Internet [?]

Those who are following this story will already know that the samples from U2's new album were not "siphoned off" along cables feeding the band's own video camera", that provides a one day delayed view of U2's studio activities, but were copied from a promotional video that was sent out from Island Records to their office in Hungary. The video was reported to have been borrowed and samples taken from it - a purposely degraded recording - were uploaded to a web page on the Internet.

The story seems to have got very quickly elaborated to include hackers. The hacker aspect appears to have come from the quote in the Sunday Times from a "former hacker":

Hackers may have used the camera as a door into the studio's computers where the new songs are stored.

The real risk here is that it seems that newspapers don't employ anyone qualified to proofread and follow up their Internet related stories. (Also c.f. the recent Observer story about pornography on the Internet).

✶ The SEI Conference on Risk Management

Carol Biesecker <cb@SEI.CMU.EDU>

25 Nov 1996 20:30:22 GMT

The SEI Conference on Risk Management: Managing Uncertainty in a Changing

World April 7-9, 1997, The Cavalier Hotel, Virginia Beach, Virginia.

Planned in cooperation with the Society for Risk Analysis, the IEEE Computer

Society, the Hampton Roads SPIN, and the Best Manufacturing Practices

Association; cooperation with Software Program Managers Network is pending.

[Featured renowned keynote speakers, distinguished presenters, contributed

presentations, papers, tutorials, workshops...]

For additional information about the conference, contact

SEI Customer Relations, Software Engineering Institute

Carnegie Mellon University, Pittsburgh, PA 15213

Phone, Voice Mail, and On-Demand FAX 412 / 268-5800

Customer-relations@sei.cmu.edu

World Wide Web: <http://www.sei.cmu.edu>

Event Registration: Contact

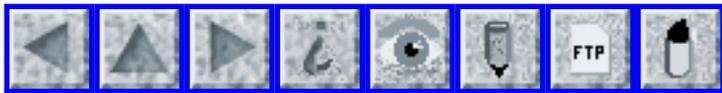
Events, Software Engineering Institute

Carnegie Mellon University, Pittsburgh, PA 15213-3890

Phone, Voice Mail, and On-Demand FAX 412 / 268-7388

FAX 412 / 268-7401

Internet registration@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 18: Issue 64

Monday 2 December 1996

Contents

- [Amtrak ticket system breaks down](#)
[PGN](#)
- [Bell Atlantic/Northern Telecom upgrade failure](#)
[Christopher Palermo](#)
- [Shetland Islands newspaper hyperlink controversy](#)
[Lance Hoffman](#)
- [RISKS of misidentified versions](#)
[John Pelan](#)
- [Risks not limited to technology](#)
[Rich Mintz](#)
- [Czech hackers allegedly rob banks](#)
[Mich Kabay](#)
- [Data diddling in cockroach races](#)
[David Kennedy](#)
- [Scary spelling correction](#)
[Geoff Kuenning](#)
- [Web-based auto update of Microsoft's Java support](#)
[Tim Panton](#)
- [E-mail solicitation on the rise](#)
[Scott C. Savett](#)

- [ATMs zapped](#)
[Bruce Wampler](#)
 - [Radiation and crypto](#)
[Jean-Jacques Quisquater](#)
 - [Re: Smart cards and radiation](#)
[Jean-Jacques Quisquater](#)
 - [Workshop on Human Error and Systems Development](#)
[Nancy Leveson](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ **Amtrak ticket system breaks down**

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

Sun, 1 Dec 96 20:04:04 PST

On Friday, 29 Nov 1996, Amtrak's nationwide reservation and ticketing system bellied up during what is usually the heaviest travel weekend of the year. The outage caused enormous confusion and delays, because agents typically had no printed schedules and fare tables. [Source: An item from *The New York Times* in the *San Francisco Chronicle*, 30 Nov 1996, A6.]

⚡ **Bell Atlantic/Northern Telecom upgrade failure**

Christopher Palermo <cpalermo@next.com>

26 Nov 1996 21:09:34 GMT

Bell Atlantic Customers Put on Hold by Directory Assistance
[Source not specified, 26 Nov 1996. PGN Abstracting.]

Hundreds of thousands of would-be telephone callers in nine states from NJ

to WV could not get prompt directory assistance from Bell Atlantic on 25 Nov 1996, because of flaws in new database software installed by Northern Telecom that affected the entire customer area. The problems affected all of the about two dozen directory-assistance centers throughout the day, until the old version could be resuscitated. Operators were noting requests and calling customers back when assistance could be attained (with delays typically from three minutes to half an hour). Northern Telecom said that the new upgrade was intended to correct some minor errors in the earlier version, and had previously been used without incident by at least two other large telcos. Blame was allocated to a technician who had installed the software. This was reportedly one of the biggest outages of this kind ever.

✶ Shetland Islands newspaper hyperlink controversy

hoffman <hoffman@seas.gwu.edu>

Sat, 30 Nov 96 08:43:11 -800

The Shetland Islands have a 124-year-old print weekly (**Shetland Times**) and a 1-year-old online daily (**Shetland News**). The **News** includes titles of **Times** articles as hypertext links to the **Times**. Robert Wishart, the **Times** managing director (who once fired his former editor, Jonathan Wills, who is now the **News** publisher), has demanded that the links be removed; Wills has refused, although he did add asterisked footnotes. Wishart then

invoked Scotland's Court of Session, which issued an interim interdict against the hyperlinks. A full hearing is pending. If the interim judgement is upheld, this is seemingly a landmark case in Scotland and potentially the UK, including issues such as the differences between a web site and a cable TV service, and whether newspaper headlines constitute copyrightable literary works. [Source: Scottish Case Tests 'Right to Link', By Pamela Mendels, *The New York Times* CyberTimes, 30 Nov 1996. PGN Abstracting] <<http://www.nytimes.com/library/cyber/week/1130shetland.html>>

[So, perhaps the *Times* really wants the *News* to stop a little horsing around, and pony up? But the ponies are so small there. PGN]

⚡ RISKS of misidentified versions

John Pelan <johnp@am.qub.ac.uk>
Wed, 27 Nov 1996 00:33:32 +0000 (GMT)

A recent security announcement was made to the 'linux-alert' security list describing how the 'lpr' utility suffers from the (now infamous) buffer overrun problem. This could be exploited as a security vulnerability in the case where it has the suid bit set.

It wasn't until after this first announcement that it was realised that various Linux distributions have different ideas about the version number of the *same* lpr source. Of course, this could cause much

confusion and
prompted a follow-up message drawing people's attention to this
somewhat
annoying and misleading situation.

The RISKS are that, especially in the case of freely-
redistributable
source, users may not know the 'true' version that they are
running and
may be deluded into thinking that they have a 'fixed' or 'safe'
version.
Of course, the program *could* differ in all but name but in any
case
some co-ordination, clarity and careful thought should be
exercised by all.
A case for truth in advertising ?

John Pelan (J.Pelan@qub.ac.uk)

⚡ Risks not limited to technology

Rich Mintz <mintz@netresponse.com>
Tue, 26 Nov 1996 15:16:33 -0500

The following item from WhiteBoard News (posted without
permission of
the author joeha@microsoft.com; for list info,
<http://www.vantagepoint.com/ghayes/Lists/news.html>) reminds us
that
risks are possible in the case of any system that's relied upon,
whether or not that system is technological in nature:

== begin excerpt ==

Jackson, Tennessee: Cathy Mullikin's bird is cooked, and her
calendar is
toast. Mullikin had her Thanksgiving turkey dinner already
cooked on
Thursday [Nov. 21], "and my friends and family are coming on the

28th and
they're going to think I'm a kook," she said.

She should never have believed that free calendar. Jackson-Madison County General Hospital gave out 40,000 of them last year and every last one said Thanksgiving was on the 21st instead of the 28th. "I wouldn't have known it was wrong except my niece called and asked what I was doing. When I told her I was finishing up Thanksgiving dinner, she said 'A week in advance?'" Mullikin told The Jackson Sun on Thursday.... "We've had a number of calls from people who have seen the error and called it to our attention," [JMCG Hospital] spokesman Ken Marston said.

[Various power outages were reported on Thanksgiving Day, when it was stormy and windy in parts of the western U.S. Many turkeys apparently were left partly cooked during the outages. PGN]

⚡ Czech hackers allegedly rob banks

Mich Kabay <75300.3232@CompuServe.COM>
27 Nov 96 16:08:25 EST

>From "Central & East European Secure Systems Strategies (CEESSS)" with permission of the copyright holder:

Secret incidents of hackers' attacks upon Czech banks and release of Czech citizens' personal information by Steven Slatem <sslatem@intellitech.cz>
Copyright (c) 1996 IntelliTech

Hackers stole 50 million Kc (\$1.9 million) during

attacks upon unnamed Czech banks and, in another incident, obtained and posted to BBSs a file of Czech citizens' personal information, we learned in an interview at INVEX (Brno, 22 -- 26. October) with Jiri Mrnustik, CEO of the Brno-based anti-virus and encryption software developer AEC s.r.o.// (ss961112-002) (630 words) (STS)

Central & East European Secure Systems Strategies (CEESSS) is delivered via e-mail and the Web. See <http://www.intellitech.cz/ceesss/> for details.

[To preempt our esteemed moderator, I will immediately warn readers that the facts will have to be Czeched before giving credence to this report.]

M. E. Kabay, Ph.D. / Director of Education
National Computer Security Association (NCSA) / <http://www.ncsa.com>

⚡ Data diddling in cockroach races

David Kennedy <76702.3557@CompuServe.COM>
25 Nov 96 23:51:06 EST

Criminal group made money by manipulating ...
COMTEX Newswire 25 Nov 1996

SARATOV, November 25 (Itar-Tass) -- A well-organised criminal group that made more than 800 million roubles every month by manipulating computer files in gambling has been exposed by police in the Saratov region, the middle Volga. A source in the regional directorate in charge of fighting organised crime told Itar-Tass that computer-added swindling was

exposed by
police for the first time in Russia, although crimes of this
sort have been
reported in many regions of Russia. The source described the
technology of
fraud: the operator used a false file to influence the outcome
of the
"cockroach races" in a way that ensured that the victory was won
by the
cockroach chosen by the operator. [Or perhaps the file was
altered to
select the designated "winner"? PGN]

The experience accumulated in the process reportedly will enable
the law
enforcers in other regions of Russia to take into account
computer swindlers
who have escaped responsibility until now. (The net take was
about US\$5,500
daily.)

Dave Kennedy [CISSP] Research Team Chief, National Computer
Security Assoc.

🔥 Scary spelling correction

Geoff Kuenning <geoff@ficus.cs.ucla.edu>
Wed, 27 Nov 1996 10:55:20 -0800

Here's a verbatim quote from the Orchestra List, which is
occupied by
musicians and conductors. Apparently spelling correctors are
getting
RISKier all the time. Note that this was *automatic* spelling
correction,
so apparently the user didn't even get a chance to override the
incorrect
decision.

> Subject: Parts are a MESS

...
> >Here's a warning on the E.C. Scarier parts to the Mozart
Vespers, K. 321.
> In
>
> Well, I typed E.C. S-c-h-i-r-m-e-r. I must figure out how to
disable my
> automatic spell correcting program so it doesn't do this to me
again. But
> then again, given the condition of the parts, maybe scarier is
the better
> term anyway.

Geoff Kuenning g.kuenning@ieee.org geoff@ITcorp.com
<http://fmg-www.cs.ucla.edu/geoff/>

[But a MASS is a MESS(E) (in German, French) is AMISS (from
Latin, MISSA).

You'll have to vesper more softly ven you perform. PGN]

🔥 Web-based auto update of Microsoft's Java support

Tim Panton <tpanton@ibm.net>
Wed, 27 Nov 1996 11:18:20 +0100

[Here is a frightening snippet from Microsoft's website I'm
not sure I
understand the full implications of it, but I don't doubt that
there are
risks involved.]

<http://www.microsoft.com/java/sdk/getstart/javac007.htm> :

Updating the Java Support on a User's Machine

If you are placing an applet that uses COM on an HTML page
accessible from
the Internet, you must ensure that any users who encounter that
page have a

version of the Java Support for Internet Explorer that fully supports Java/COM integration.

To do this, you must insert the following tag on the HTML page containing your applet (or on the introductory page of your Web site):

```
<OBJECT  
CLASSID="clsid:08B0E5C0-4FCB-11CF-AAA5-00401C608500"  
CODEBASE="http://www.microsoft.com/java/IE30Java.cab#Version=1,0,0,1">  
</OBJECT>
```

This tag causes the user's Internet Explorer to check the version of its Java support. If the version installed on the user's machine is not up-to-date, Internet Explorer downloads the latest version of Java support from <http://www.microsoft.com> and updates the user's machine.

- - - -

The potential risks are endless. Say I know of a security hole in a specific version of IE, I can automatically get visitors to my website to install it, then attack them through the hole.

Some questions:

Does it ask the user first ?

Can I force a 'down'grade, i.e., install an older version ?

What happens if the user uses two sites that require different versions?

Is the code signing strong? (i.e., stronger than MS's CD keys ?), can I fake a CAB file?

Tim Panton, Westhawk Ltd, Frederik Hendriklaan 89, 2582BW Den Haag. The Netherlands tpanton@ibm.net +31 6 5348 1795 <http://www.westhawk.co.uk>

✶ E-mail solicitation on the rise

"Scott C. Savett" <ssavett@CLEMSON.EDU>

Fri, 29 Nov 1996 18:30:06 -0500

I'm sure we're all increasingly aware of annoying unsolicited commercial e-mail messages forced into our electronic inboxes. But is this just the tip of the iceberg?

A mass mailing recently ended up in my e-mail, promising e-mail marketing to 100,000 or 1,000,000 people for \$195 or \$995 respectively. Ominously, the message did not have a valid "From:" address in the header, and was passed through at least two servers before being distributed to an undisclosed list of recipients. Does a \$100 InterNIC registration and \$15/month ISP charge now give anyone the ability to saturate the Internet community with unsolicited e-mail?

Besides carefully screening incoming e-mail, what recourse does one have against acts of e-mail terrorism? With many SMTP e-mail servers readily accepting mail from anonymous senders, how can we stop the constant stream of unsolicited commercial e-mail being forced down our throats? This trend gravely concerns me, as it should concern us all!

Scott Savett, Graduate Student in Analytical Chemistry, Clemson University
Webmaster, National Collegiate EMS Foundation <http://www.ncemsf.org/>

⚡ ATMs zapped

<wampler@cs.unm.edu>

Fri, 29 Nov 1996 14:24:33 -0700 (MST)

Last week I was unable to use my cash card to pay for my groceries at the local grocery store because the system wasn't working. The November 28, 1996 business section of the Albuquerque Tribune explained why:

"ATMs zapped: First Security's Albuquerque-area automated teller machines and electronic funds-transfer stations at Smith's Food & Drug Stores went on the blink last weekend when a new cellular-telephone company started service using a microwave frequency that bled over to First Security's ATM and EFT frequency. Service disruptions forced Smith's to shun electronic purchases Saturday through Monday. "We apologize to our customers who were inconvenienced and are working hard to fix the problem, but the problem of jammed frequencies is just going to get worse," said Paul Bouschelle, executive vice president for First Security Bank of New Mexico."

Two obvious RISKS revealed by this incident:

1. The unintended and unexpected problems caused by bringing a new system on-line. For whatever reasons, this problem took the whole weekend to resolve.
2. This article also reveals that the ATMs and EFT terminals communicate over microwave frequencies, and are thus subject to being tapped or monitored, perhaps more easily than if they were connected via wire or telephone lines. I guess I've assumed that most of these terminals were

handled via phone line, which seems inherently more secure than a radio link. This may not be true. I don't recall much discussion in this group of the risks of using radio links vs. wire for financial data transfer.

Bruce E. Wampler, Ph.D., Adjunct Professor, Department of Computer Science,
University of New Mexico wampler@cs.unm.edu <http://www.cs.unm.edu/~wampler>

⚡ Radiation and crypto

Jean-Jacques Quisquater <jjq@dice.ucl.ac.be>

Mon, 02 Dec 96 09:23:18 GMT

Your electronic wallet in the Van Allen radiation belt, or Electronic commerce at RISK in space?

Jean-Jacques Quisquater
UCL Crypto Group - Microelectronics Lab
November 30, 1996

[Note: This short remark was intended as a contribution to the rump session of EUROCRYPT '97 but the subject is too hot to wait.]

>From end September until now many announcements were issued about the so-called Bellcore attack against tamper-resistant chips (example: smartcard or chipcard for electronic commerce). The attack is based on the (theoretical) possibility of flipping some bits (at some random position) of the secret key, stored in RAM or E2PROM, before or during the computations done by the chip. Another attack is to induce some decoding error during the execution of one instruction (Anderson and Kuhn).

One crucial question is the effectiveness of such attacks by malicious hackers. In fact, this problem was very well studied in the contexts of nuclear physics and of space applications (what about the behavior of semiconductors in such hard environments?). In that area, there is the concept of SEE (Single Event Effect) and it is what we are trying to study!

A SEE is an event induced by radiation, temperature, microwave, ..., having some effect one time on a device. There are many studies about that. What we need to know are the SEEs --- relatively well focused (one or few bits are flipped), --- and/or at a given moment, --- and/or for a very short time.

Here are some references to begin the study. The reference newsgroup is sci.engr.semiconductors (others?).

- The NASA ASIC guide, published by JPL and NASA, Chapter 4, Design for radiation tolerance, 1993.
- Hardening integrated circuits against radiation effects, J.-P. Colinge and P. Francis, November 1996, Notes (66 pp.), Microelectronics Lab, UCL, Louvain-la-Neuve, Belgium (yes!, my lab),
- Single-Event-Effect mitigation from a system perspective, IEEE Trans. on Nuclear Science, vol. 43, April 1996, pp. 654-660.
- Laboratory tests for Single-Event Effects, IEEE Trans. on Nuclear Science, vol. 43, April 1996, pp. 678-686.
- Microbeam studies of Single-Event Effects, IEEE Trans. on Nuclear Science,

vol. 43, April 1996, pp. 687-695.

- Soft errors susceptibility and immune structures in dynamic random access memories (DRAM's) investigated by nuclear microprobes, IEEE Trans. on Nuclear Science, vol. 43, April 1996, pp. 696-704.
- 32-bit processing unit for embedded space flight applications, IEEE Trans. on nuclear science, vol. 43, June 1996, pp. 873-878.
- Single Event Effect testing of the Intel 80386 family and the 80486 microprocessor, IEEE Trans. on Nuclear Science, vol. 43, June 1996, pp. 879-885.
- Analysis of local and global transient effects in a CMOS SRAM, IEEE Trans. on Nuclear Science, vol. 43, June 1996, pp. 899-906.
- 1997 IEEE nuclear and space radiation effects conference, call for papers.

Jean-Jacques Quisquater, Universite catholique de Louvain, Place du Levant,
3, B-1348 Louvain-la-Neuve, Belgium tel 32.10.47.25.41 jjq@dice.ucl.ac.be

✉ Re: Smart cards and radiation

Jean-Jacques Quisquater <Quisquater@dice.ucl.ac.be>
Mon, 2 Dec 1996 19:39:49 +0100 (MET)

A (corrected thanks to Arjen Lenstra) postscript version of
Attacks on systems using Chinese remaindering
by Marc Joye and Jean-Jacques Quisquater, Report CG-1996/9

is accessible at the following URL:

<http://www.dice.ucl.ac.be/crypto/techreports.html>

✈ Workshop on Human Error and Systems Development

Nancy Leveson <leveson@cs.washington.edu>

Mon, 02 Dec 1996 02:33:56 PST

Workshop on Human Error and Systems Development

The Senate Room, University of Glasgow

20-22 March 1997

Co-chairs: Nancy Leveson and Chris Johnson

<http://www.dcs.gla.ac.uk/~johnson/HF_Engineering.html>

Recent accidents in a range of industries have increased concern over the management and control of safety-critical systems. Much recent attention has focussed upon the role of human error both in the development and in the operation of complex processes. This workshop will, therefore, provide a forum for practitioners and researchers to discuss leading edge techniques that can be used to mitigate the impact of human error on safety-critical systems.

Our intention is to focus the workshop upon techniques that can be easily integrated into existing systems engineering practices. With this in mind, each day will have a different theme. The session on Thursday 20th March will focus on accident analysis and risk assessment techniques. Friday, 21st will focus more narrowly upon interface and component

design,
development, and testing. We also encourage papers that cross
these
boundaries.

Saturday 22nd March will provide the opportunity for informal
discussion
about the issues raised during the workshop. The day will be
spent on the
Isle of Arran, off the west Coast of Scotland [not to be
confused with
Aran].

Deadlines: Authors should submit extended abstracts to Chris
Johnson, see
below, to arrive no later than January 17th, 1997. [<see http...
>]

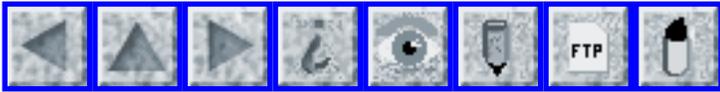
Programme Committee:

Veronique de Keyser, University of Liege, Belgium.
Chris Johnson, University of Glasgow, Scotland.
Peter Ladkin, Universitat Bielefeld, Germany.
Nancy Leveson, University of Washington, USA.
Chris Mitchell, Georgia Institute of Technology, USA.
Kim Vicente, University of Toronto, Canada.
David Woods, Ohio State University, USA.

Further Information:

Chris Johnson, Department of Computer Science,
University of Glasgow, Glasgow, G12 8QJ, Scotland.
johnson@dcs.glasgow.ac.uk
tel.: +44 141 330 6053 fax.: +44 141 330 4913

This workshop is organised by the Glasgow Accident Analysis
Group,
Department of Computing Science, at the University of Glasgow.
It is
supported by the Human Factors section, IT and Computer Science
programme
within the UK Engineering and Physical Sciences Research Council.



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 18: Issue 65

Monday 9 December 1996

Contents

- [Limits of automated newsgathering](#)
[Terry A. Ward](#)
- [Crypto to protect ``bomb" throwers](#)
[Peter Wayner](#)
- [Another banking system hits the dust](#)
[John C. Bauer](#)
- [Software hunts and kills Net viruses](#)
[Hans A. Rosbach](#)
- [Don't touch this switch!](#)
[Rick Simpson](#)
- [Blown Fuse Takes Out 911 System](#)
[Scott Lucero](#)
- [Web content-substitution attack was a proxy-server fault](#)
[James Cameron](#)
- [Risks of inappropriate encouragement](#)
[David M. Chess](#)
- [Reuters computer tech brings down trading net](#)
[Steve L](#)
- [Combatting cookies](#)
[Simson L. Garfinkel](#)

- [MS-Access Runtime trashes WFW](#)
[Bob Price](#)
 - [Snowjob in selling computer books](#)
[Al Donaldson](#)
 - ["Computer errors cause several plane crashes"](#)
[Martin Minow](#)
 - [RISKS of frequent-flier long-distance promotions](#)
[Jonathan Clemens](#)
 - [Year 2000 and expiration dates](#)
[Robert Nicholson](#)
 - [Centralized computing](#)
[Darin Johnson](#)
 - [Re: Bell Atlantic 411 outage](#)
[Robert J. Perillo](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ Limits of automated newsgathering

"Terry A. Ward" <terrywa@ix.netcom.com>

Wed, 4 Dec 1996 11:35:55 -0800

I subscribe to the NewsPage Direct automated news service and a recent selection in HUMAN SEXUALITY highlighted the risk of confusing a rugby position with a sex-workers position:

>> RUGBY UNION-CANADIAN HOOKER OUT IN THE COLD - Canadian international

hooker Karl Svoboda has been ousted from the Oxford team to face

Cambridge University in the showpiece Varsity match at Twickenham

next Tuesday. (Reuters)

[This is a scrum-ptious item! TNX. PGN]

🔥 Crypto to protect ``bomb" throwers

Peter Wayner <pcw@access.digex.net>

Mon, 9 Dec 1996 18:07:30 -0500

The Washington Post (6 Dec 1896) reported that a radio and television broadcast of the annual Army/Navy football game would be distributed to many of the ships at sea in "encrypted" form. The signal would be used to boost morale, although the encryption may ruin morale for the folks stationed at NSA/DIA listening posts. But perhaps the algorithm will be simple enough to be part of the challenge for them.

Of course, the automatic word scanners are sure to light up when words like "bomb" and "blitz" come over the air.

I wonder if they sign the broadcast with a digital signature to make sure an authentic version reaches the troops? Spoofed versions would be true info warfare. The enemy could ensure that both divisions would be demoralized by feeding a doctored version to the winning side. But then there is still the RISKS of the Air Force, who are in the big-bomb delivery department.

[Incidentally, for non-U.S.-football devotees, a "bomb" is a long pass, and a "blitz" is an extra-man defensive attack. I suppose "getting sacked" has multiple meanings in an Army-Navy game. PGN]

✶ Another banking system hits the dust

"John C. Bauer" <jcbauersyseng@igs.net>

Mon, 2 Dec 1996 14:38:39 -0500

On 30 Nov 1996, the Canadian Imperial Bank of Commerce Interac service was

victimised by its attempted software upgrade, affecting about half of all

would-be transactions across eastern Canada. [Source: Debit card failure

angers customers, by Colin Freeze, Citizen Correspondent, The Ottawa

Citizen, 2 December 1996, Ottawa, Ontario, Canada. PGN Stark Abstracting]

One business affected was Loblaw's, a grocery chain. Grocery stores do not

accept credit cards. (My wife Ann says it may be a provincial law.) I can

just see someone with a cartful of groceries arriving at the checkout and

being asked for cash they are not carrying.

As of 1 p.m. EST, 2 Dec 1996, the local branch of the bank had no statement

to give to customers! Will this be touted as another example of computer

people living outside the real world, where shopping is at a peak on

Saturday afternoons, especially near Christmas?

✶ Software hunts and kills Net viruses

Hans A. Rosbach <haro@sesam.dnv.no>

02 Dec 1996 18:52:31 +0100

The Sunday Times (1 Dec 1996) wrote:

Software hunts and kills Net viruses

VIRUS-KILLING computer software that uses artificial intelligence to find and destroy new viruses is to be set loose on the Internet by IBM next week.

The software, originally developed to play backgammon, will spread itself through the Net over the next year, learning how to kill new strains of virus as it goes. According to Gregory Sorkin, a researcher at IBM's Watson research laboratory, the system will be far more successful than humans at fighting computer viruses. "Once it learns the viruses already out there, the system will even be able to predict what new viruses will appear, and work out ways of stopping them before they even exist," says Sorkin. The system uses temporal difference, a method which relies on the computer looking for patterns within virus software, rather than individual lines of program code.

If I understand it correctly, this is software that will spread itself on the net, adapt itself, and destroy other things on the net.

How can something like this be tested? How can we be sure that the technology behind it will not be used to create the next generation of viruses? I find this scary.

Hans Amund Rosbach haro@sesam.dnv.no

⚡ Don't touch this switch!

"Rick Simpson" <simpson@watson.ibm.com>

Thu, 05 Dec 96 18:13:54 -0500

Today I attended a meeting in a large office building of a Major Computer Company. As I entered the conference room, the organizer of the meeting was trying to find a way to lower the projection screen from its storage place in the ceiling. There was no cord attached, so he was searching for a switch for the screen's motor.

On the wall next to the door was a push-button switch, brightly backlit in red, with a hand-written sign that read, "Don't touch this switch." (Also scribbled on the sign, in another hand, was "Don't touch" in Spanish.) The organizer seemed to think this might control the screen, so he pressed the button. Needless to say, the screen did not descend. The ventilation fans went off, though.

Several minutes later, a fellow poked his head in the door and asked, "Did someone touch that switch?" [Just like in a cartoon, isn't it?] "Yes," the organizer said, "we were trying to get the screen down."

"Don't touch the switch," said the man in the door, "It turns off the computer room next door."

The conference room was evidently once part of a raised-floor machine room, and the Emergency Power Off switch next to the door is still active.

The RISKS, I submit, are too obvious to list.

Rick Simpson IBM T. J. Watson Research Center Yorktown Heights, New York

simpson@watson.ibm.com

⚡ Blown Fuse Takes Out 911 System

lucero <lucero@optec.army.mil>

Tue, 03 Dec 96 05:21:48 EST

National Public Radio reports that a blown fuse took out a large portion of Iowa's 911 emergency phone system for three hours over the Thanksgiving weekend. U.S. West could not say how many 911 calls went unanswered. A spokesperson said that the troubles isolating the problem came from the complexity of the system. The RISKS are pretty evident.

Scott Lucero U.S. Army Software Metrics Program

⚡ Web content-substitution attack was a proxy-server fault

James Cameron <cameron@ripper.stl.dec.com>

Tue, 3 Dec 1996 14:05:50 +1100

I heard from a friend a detailed account of an apparent content substitution attack on his corporate web server that highlights a couple of risks. With his permission I have summarised the order of events:

- A few days ago, a sales person employed by the company reported a

- pornographic image had replaced the corporate logo on the main page.

- A correct logo was downloaded to the server within minutes,

- but
before saving the existing image, thus erasing the evidence.
- Research showed a known defect in the operating system code that
can be exploited to yield root access by remote users. Tests showed
that the firewall and web server were vulnerable. Patches were
obtained and installed to remove the vulnerability. Much effort.
 - Conflicting data from logs appeared. The web server logs showed
that the image had not been replaced. Firewall logs agreed. Web
proxy server logs claimed otherwise.
 - The pornographic image was found in the web proxy server cache,
with a different URL, using a search by file size, and the logs
confirmed that it had been viewed by users within the company.
 - No evidence was found to prove that a break-in had occurred.

The staff deduced that the web proxy server had somehow mixed the pointers
to the cached images, and had returned the incorrect image to the internal
users. No reports were received from Internet users.

Risk: a web proxy server may change your view of the Internet, and may cause
you to waste considerable time tracing a break-in that didn't happen.

Risk: allowing staff full access to the web increases the chances of a file
mixup causing disturbance.

Also, there were no controls to ensure that CERT notifications were integrated

into the firewall configuration. It took a suspected break-in before a search was made for vulnerabilities.

James Cameron (cameron@stl.
dec.com)

Digital Equipment Corporation (Australia) Pty. Ltd. A.C.N. 000
446 800

⚡ Risks of inappropriate encouragement

"David M. Chess" <CHESS@watson.ibm.com>

Wed, 4 Dec 96 10:39:13 EST

My daughter has a few multi-media-type CD-ROM games, and they are to various degrees cute / cuddly / talkative / friendly. The most talkative and friendly one has one very annoying and counterproductive habit. In the find-the-hidden-objects puzzle, the little voices on the speakers say happy / reassuring things every time you click the mouse on a place where there's no hidden object. "Try again!" "Nope, not there!" and so on. The encouraging phrases are as far as I can tell picked at random. Unfortunately, some of them have *semantics* beyond just "Try again".

The most annoying ones are "Ooh, not quite!" and "You're getting closer!".

Because they're generated just at random, the voices can say "Ooh, not quite!" when the player is clicking as far as possible from the target, and can say "You're getting closer!" when in fact you're getting further away.

My daughter learned to ignore the semantics of these messages very quickly

(the plasticity of youth), but when looking over her shoulder I still find them annoying and misleading, and have to remind myself that they're meaningless.

The general tendency, the risk category, is a familiar and important one: computers that talk seem from the outside to know what they're saying, whereas the people who've made them talk may not really have thought it through at all, and the programs themselves can be arbitrarily stupid.

(Another similar program will say encouraging things like "Your eyes are as sharp as the eagle's" when the child finally gets all the rolling targets in the archery game, even if the player is far beyond the age-appropriate difficulty level, and has been struggling for many minutes to hit each one. Another, related, risk that reaches far beyond computers: overgenerous praise...)

David M. Chess High Integrity Computing Lab IBM Watson Research
<http://www.av.ibm.com/> <http://www.research.ibm.com/massive>

⚡ Reuters computer tech brings down trading net

<stevel@mcgraw-hill.com>

Mon, 02 Dec 96 16:02:11 EST

Dealing rooms sabotaged by HK Reuters technician
By Nicholas Denton in London and John Ridding in Hong Kong, 29
Nov 1996
Financial Times Limited

A disgruntled computer technician at Reuters in Hong Kong has caused the financial-information provider deep embarrassment by sabotaging the dealing-room systems of five of the company's investment bank clients.

The attack crippled for up to 36 hours the computer systems bringing market prices and news to traders at NatWest Markets, Jardine Fleming,

Standard Chartered, and two other banks. The banks, which resorted to alternative terminals such as Bloomberg, claimed the tampering had no significant impact on trading and said neither they nor their clients had experienced losses as a result.

The incident was reportedly the most serious breach of security disclosed in Reuters' corporate history, and is causing some rethinking of privileges.

The maintenance engineer in question has been suspended. He apparently visited the client sites and initiated deferred commands to subsequently delete specific operating system files.

Combatting cookies

"Simson L. Garfinkel" <simsong@vineyard.net>

Tue, 03 Dec 1996 08:25:13 -0500

I've been thinking a lot about (web) cookies lately. One of the problem with the current situation is that you basically have two choices with the User Interface that both Netscape and Microsoft have created for your

browsers:

1. You can simply accept all cookies.
2. You can have your browser warn you every time a cookie is sent your way and have the option of accepting it or not.

A cookie, for those not in the know, is a little tarball of data that gets sent to your browser. Cookies can be used to track users, by keying their browsers to a database. Or they can be used to preserve privacy, by storing private information on the user's browser, rather than on the web server.

Right now, a cookie gets sent to your browser whenever you get an HTTP response with the words "Set-Cookie:" in the header. After that, whenever you contact the web site, you send the cookie back.

It seems to me that an excellent way to deal with the cookie problem would be to have more user interface options:

- * Simply do not accept cookies.
- * Specify who you will accept cookies from, and who not.
- * Accept cookies, but do not send them back.
- * Have a decent user interface to show which cookies you have and how often they are used. Let you delete them individually, rather than just all or nothing.

I've written more about cookies in an upcoming article for HotWired. It will appear at <http://www.packet.com/garfinkel> on Wednesday, 11 Nov 1996.

⚡ MS-Access Runtime trashes WFW

<Bob.Price@cwi.cablew.com>

Tue, 3 Dec 1996 13:25:24 -0500

Unless especial pains are taken, 16-bit MS-Acess runtime disks made on a Windows-95 machine with 16-bit Access will cause near-irreparable harm when installed on a WFW or Windows 3.1 machine. The reason is that some 32-bit system .DLLs are copied to the distribution diskettes (or network distribution set) along with the 16-bit files, and because the 32-bit files have the same names as the 16-bit files, the 16-bit platform no longer works properly. I'm told the official Microsoft paper on the subject says to format the hard drive and re-install everything. I was able to "recover" by upgrading to Windows-95; others have had success ferreting out the specific files and replacing them. Reinstalling WFW didn't fix anything.

Bob Price Cable & Wireless Inc. bobp0303@hotmail.com (703)760-3071

⚡ Snowjob in selling computer books

Al Donaldson <al@escom.com>

Tue, 3 Dec 96 14:43:48 EST

January 1996 was a snowy month in Virginia. We were hammered by a storm on the 6th that dropped about two feet of snow, and closed everything (that wasn't already closed) for a couple of days, followed by another storm on the 12th that gave us another 8 or 10 inches.

So that Friday (12th), I spend most of the afternoon shoveling out my driveway. Then, remembering that I needed to buy a book to prepare for some computer work that weekend, I called my favorite technical bookstore to see if, by some chance, they might be open that night. (I didn't really expect them to be open, but it was worth a try...)

Sure enough, someone answered, so I asked how late they would be open.

"Nine o'clock," was the answer. I confirmed the closing time, perhaps still not really believing they'd be open, then drove my 4WD truck about 15 miles on snowy roads to get there. But when I arrived around 8:00pm, the store was quite obviously closed.

That evening I sent off a letter of protest to the store management, who responded the following Monday that the *Virginia* store had been closed all day because of the heavy snow, and they'd forwarded the phones over to one of their California stores.

✶ "Computer errors cause several plane crashes"

Martin Minow <minow@apple.com>

Fri, 6 Dec 1996 17:15:03 -0800

>From an article in the Swedish newspaper, Aftonbladet, Dec 6, 1996

written by Claes Thunblad. <http://www.aftonbladed.se/nyheter/dec/06/flyg.html>

[[Note: while the Swedish translations I send to RISKS are usually from *Svenska Dagbladet*, one of the two "newspapers of record," this is from an evening tabloid, and should be understood as such. If you imagine my other translations as originating from *The New York Times* or *Daily Telegraph*, think of this as from the *New York Post* or *Evening Standard*. I've tried to be both accurate and true to the tone of the article. I've translated a bit more than 50% of the article, but omitted the sidebars listing recent air accidents. Swedish typographic conventions make it difficult to precisely mark quotations, and I apologize for any errors.]]

The advanced computer systems developed to improve flight safety have become a death trap. "Pilots can no longer keep track of everything," says Per-Olof Sk=F6ld, president of the Swedish pilot's organization. [[In bold-face on the web page.]]

"We've discussed this problem on several occasions. The critical point is when the computer system should be disconnected; when the pilot stops being a passive monitor of the system and becomes an active operator," says Sven-Eric Sigfridsoson of the national air accident commission.

The new advanced technology in airplanes was developed by technicians and engineers. They're the ones who test-fly the system before the plane is put into traffic.

"These things were designed by engineers and technicians are not always pilot-friendly. Today there are several automatic sequences that

pilots can never keep track of," says Per-Olof Skold. ... The pilot's nightmare scenario is that the technology will get even more advanced. That's what the technicians want.

✈ RISKS of frequent-flier long-distance promotions

Jonathan Clemens <jclemens@aa.net>

Tue, 3 Dec 1996 11:56:58 -0800 (PST)

Several years ago, a local long distance carrier began a program offering one frequent flier mile for each minute of long distance calling. My sister signed up for the program, but later moved and disconnected that particular phone line.

However, recently she began receiving program statements again. It seems that number has been reissued, and the new owners have this long distance carrier, but have NOT signed up for the "Mile-A-Minute" program.

When reassigning a number, all features should have been reset to their defaults. In this case, they were obviously not. The total 'cash' value (at \$.03 per mile) of the error is not very significant. A more serious risk is that my sister receives a detailed billing report every month, listing the number called and the call duration for each qualifying number. It is sent to the address listed on her frequent flier account, and not to the billing address of the new owners of the line.

In addition to eliminating 'old' data, such systems need to take into account the nature and sensitivity of data disclosed on such statements.

Jonathan Clemens, jclemens@aa.net

⚡ Year 2000 and expiration dates

<robert@justine.dgsys.com>

Sat, 7 Dec 1996 19:35:02 +0000

Today, I had my first encounter with the year 2000 problem. I took my shiny new, already activated, Visa cheque card into Citibank, Manhattan branch and after inserting the card into the validation machine the teller told me my card had expired. My expiry date is 01/00. A few moments later I had successfully convinced that teller that the card couldn't have been issued in the 1800's and so he phoned a verification service to check. That service also declined the card. It wasn't until I had called my own bank and asked them to turn off all security checks on the card that I could successfully obtain my cash advance.

I had earlier dismissed all the hype surrounding the year 2000 problem thinking that most corporations would have already made the necessary changes to cope. Considering it's typical for cards to be issued for 4 year periods it's not surprising to see a card issued in 1996 suffering this problem. I can only hope things improve as we approach 2000.

Robert Nicholson <robert@elastica.com>

✶ Centralized computing

Darin Johnson <darin@connectnet1.connectnet.com>

3 Dec 1996 18:43:51 GMT

A few months back, I was shopping at a Computer City, a large chain of PC stores of the sort that caters to the mass market. When I got to the front of the checkout line (which is normally slow to begin with), things came to a halt. Apparently, all transactions were handled by computer, and it was down.

OK, I thought they've got a backup in the back, and it'll kick in, or the thing will reboot. No good. After awhile, one of the clerks reported that the computer that was down was in LA (I was in San Diego). All their transactions were being handled remotely, and for all the computers and manpower they had locally, they couldn't do anything but wait.

Later still, someone came back up front with a book describing how to do checkouts manually. None of the clerks knew. When I was checked out, it took four people, one to be in charge, one to use the calculator to compute tax and total, one to verify my credit card, and one to read the instruction book.

I was struck by two ironic facets of all this. First, the reliance upon

centralized computers. The PC got its big start and popularity run initially by allowing independent computer use away from centralized MIS departments. Have things come full circle again, away from independent computers to centralized ones? It would not have been unreasonable for a computer seller to have an extra backup computer in back, something to process transactions locally and then transmit them remotely later. Perhaps the risk here is forgetting history (not to stereotype too blatantly, but I see a distinct lack of historical computer knowledge in much of industry).

The second facet is the old risk of becoming too dependent upon technology. Requiring four people to check out one small purchase is excessive, and all because none were trained to do such things manually (not to stereotype too much again, but they didn't seem to be trained that well in computers either :-). On the other hand, I can go into grocery stores and have the checkers rapidly process a large purchase, knowing the price of each item; I've had other stores take only one person to fill out receipts by hand when power was out. Why would a computer store be so crippled by a remote computer being down, were they even more dependent upon technology than other stores?

Darin Johnson darin@connectnet.com

[Yes, this is an old tale for RISKS readers. But did you think a computer store would know better? PGN]

✦ Re: Bell Atlantic 411 outage ([RISKS-18.63](#))

<Perillo@DOCKMASTER.NCSC.MIL>

Wed, 4 Dec 96 14:28 EST

This was not a complete outage, but about 60% of the Bell Atlantic company's 2,000 operator's at 36 sites could not log into their automated directory system. Of the 40% that were able to access the database, lookup times went from the typical 19 seconds into minutes. The problem manifested itself about 8am on Monday November 25th, and was fixed about seven hours later by reloading the previous version of the database software. But this was the most extensive directory-assistance failure since telephone operators started using computers, affecting hundreds of thousands of customers in nine eastern states.

Originally Bell Atlantic blamed the problem on a "software glitch" in the "Nortel Directory One" database software upgraded over the weekend. Northern Telecom stated that the new software, which was meant to correct minor errors in the previous version, was being used by several large phone companies without any problems. The problem seems to have been traced to a Nortel technician who improperly installed the software on two RS/6000 servers. The incorrect installation of the main database, also somehow caused the same type of access problems on the duplicate/backup database system.

While RISKS has concentrated on software errors, installing

software into operating systems has gotten increasingly complex, usually done by non-degreed technicians and operators, following informal instructions scrawled on the back of napkins. In this case it seems that since the malfunction was load related, the technician was unaware during system checkout that the database was incorrectly installed. More scrutiny should be given to software installation, and installation procedures or possible problems. Formal procedures with Quality Assurance (QA) checklists should be used. Could automated installation programs, or problem checking software, be used to prevent or detect installation problems?

References: "Software Glitch Snarls Bell Atlantic's 411 Calls",
Washington Post, 11/26/96, page D1 .

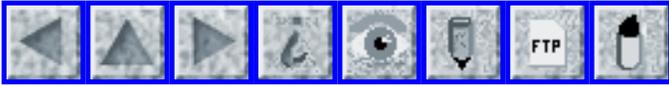
"Bell Atlantic Customers Are Put on Hold by Directory Assistance",
New York Times, 11/26/96, page A17.

"Software Glitch Hits Bell Atlantic Sites",
InformationWeek,
12/2/96, page 32.

Robert J. Perillo Staff Computer Scientist
Perillo@dockmaster.ncsc.mil



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 18: Issue 66

Thursday 12 December 1996

Contents

- [Instant money](#)
[Debora Weber-Wulff](#)
- [Digital Equipment Corp loses repetitive-strain injury suit](#)
[PGN](#)
- [RISKS of using adobe acrobat reader under Unix](#)
[Peter T. Breuer](#)
- [The risk of system administrators not understanding enough](#)
[Matt Barrie](#)
- [Denver airport baggage system simulations](#)
[Luis Fernandes](#)
- [A visit from the Goon Squad: computer evidence](#)
[Nick Brown](#)
- [Discussion of `Computer errors' causes hernia](#)
[Peter Ladkin](#)
- [re: "Plane crashes" -- corrections](#)
[Martin Minow](#)
- [Re: Aviation Accident Rates](#)
[Peter Ladkin](#)
- [Re: Don't touch this switch!](#)
[Bear Giles](#)
[Harlan Rosenthal](#)
- [4th ACM Conference on Computer and Communications Security](#)
[Mike Reiter](#)

 [Info on RISKS \(comp.risks\)](#)

 **Instant money**

Debora Weber-Wulff <weberwu@tfh-berlin.de>

10 Dec 1996 10:51:26 GMT

[from *Stars & Stripes*, 7 Dec 1996, a daily newspaper for military and such overseas. Excerpted by DWW.]

A soldier is under investigation after allegedly transferring more than a half-million dollars into his checking account from his savings account. The problem was, it wasn't his money. On 29 Nov 1996, he unsuccessfully attempted to withdraw money from his overdrawn accounts. Then he conducted a transfer of 600,000.21 from his savings to his checking account at an ATM (banks were closed for the day after Thanksgiving). Because of a defect in the ATM computer system, the transfer was completed without verification of whether funds were available in the soldier's account. Over the next few days, the soldier was able to withdraw \$300 in cash and deposited \$30,005 into a newly opened credit union savings/money market account. On 2 Dec he attempted to wire \$60,000.15 to California. Officials noticed the error and stopped the transaction. The soldier was apprehended, but has not been charged and is not in custody.

A spokeswoman for the bank said the incident was the result of a one-time glitch in the bank's computer system. An anonymous customer service representative said there have been problems with the bank's computer accounting system since 8 Nov 1996 - the day the data from Bank A was converted to Bank B [the military awards banking contracts for a limited time. They have problems at every change-over, it seems.] "From that point

on, we've just been trying to fix messes," the bank employee said, noting that the problems range from lost data to false duplication.

[I wonder if the "uneven" amounts contributed to the mess, or if it was a foul-up in general. - dww]

Debora Weber-Wulff Technische Fachhochschule Berlin, Luxemburger Str. 10, 13353 Berlin GERMANY weberwu@tfh-berlin.de <<http://www.tfh-berlin.de/~weberwu/>>

🔥 Digital Equipment Corp loses repetitive-strain injury suit

"Peter G. Neumann" <neumann@csl.sri.com>
Thu, 12 Dec 1996 10:14:46 PST

A Brooklyn federal jury awarded nearly \$6 million to three women who had sustained arm, wrist, and hand injuries apparently resulting from use of a Digital LK201 keyboard: \$5.3m to Patricia Gerassy, \$306,000 to Jill Jackson, and \$278,000 to Jeanette Rotolo. This is the first such case in which the computer manufacturer lost. Earlier cases involved Compaq and IBM. Digital will appeal. [Source: Diana B. Henriques in **The New York Times**, 10 Dec 1996, C1, also in **San Francisco Chronicle** same day, A1, PGN Abstracting.]

[Many years ago my keyboard had a very rough touch that caused severe pain in the little finger of my left hand (the **emacs** finger). I had two foot pedals installed for the control and meta keys, and the problem went away. It also helped my organ-playing technique, speaking of manual systems. But, clearly it is good advice that you should not sit at your keyboard for long unbroken sessions. Unfortunately, I don't take my own advice enough.]

⚡ RISKS of using adobe acrobat reader under Unix

"Peter T. Breuer" <ptb@it.uc3m.es>

Wed, 11 Dec 1996 20:02:03 GMT

The latest (free) beta release for linux of the adobe acrobat .pdf reader from adobe contains an interesting risk-enhancing feature, according to its documentation.

from MapTypes.pdf:

If the file cannot be opened as a PDF file, the viewer examines the UNIX file permissions. If the file can be executed by the

```
*****  
user who launched Acrobat Reader or Exchange, the viewer attempts to  
*****  
launch the file as an application. If the file cannot be launched as  
an  
*****  
application, the viewer returns an error message.
```

The risk - of death by execution - is obvious. I have to admit I haven't had time to try it. I suspect I am the only person in some radius to have time to read the documentation! I report this to you as I find it.

Peter T. Breuer, Universidad Carlos III de Madrid, Butarque 15, E-28911 Leganes SPAIN +34 1 624 9947 ptb@it.uc3m.es <<http://www.it.uc3m.es/~ptb>>

⚡ The risk of system administrators not understanding enough

SYD) <Matt_Barrie@oti.com (Matt Barrie)>

Wed, 11 Dec 1996 00:02:10 -0500

I've noticed increasingly that a lot of system administrators have placed an incredible reliance in "out of the box" security products (firewalls etc) .

These products tend to provide a fair degree of auditing and it seems that quite a few administrators don't understand what it really all means. I get the impression that the response is a typical "Quick, call Chuck, we've got a situation down here!" every time a message is logged. (Why would these security products log messages if it wasn't a threat?)

The first example is when a friend in Luxemburg e-mailed me saying that he had a new job and this was his e-mail address. He doesn't know too much about computers and asked me how I could chat to him. I asked if he was on a Unix machine, and if he had chat, we could use that. He said that he thought it was a Unix but wasn't sure - as a quick check I just telnetted quickly to his site and pressed ctrl-D as most machines tell what OS they are as a login message. The machine was TCP wrapped, but answered SunOS anyway. I guess I could have used another method to find out (nslookup etc) but this was quick & simple. It turns out that the machine was the helpdesk for a major bank of sorts - the connection spawned a return finger @mymachine - which answers for a group of local machines. It told them that five people were currently logged on to a bunch of local machines.

The log should have been read as "You had a connection attempt on port 23 which was denied - it may have come from any of these five users.."

Apparently the bank admins freaked - supposedly they had forgotten the root password the day before and read the log as something like "you have five people simultaneously breaking in to your machine from a variety of

places;
machine1.au , machine2.au , ...". They admins freaked and ran around
the
bank looking for Australians working there. They then waved logs in
their
face and asked them if they knew any of these people - any why they
would be
using all these accounts trying to break in. My friend called
frantically
from Belgium at 1am in the morning and had to send me the log so I
could
explain what it meant. Sheesh.

Another quick example comes from the fact I am the technical
administrator
for xxxx.com. We all know that spamming is on the rise - and it seems
xxxx.com is an ideal choice as a fake source domain as it is a fairly
generic sounding name. The risk is where admins who wish to stop the
spamming then go ahead and bar or send complaints to postmaster@xxxx.
com
asking for the spamming to stop - when if anyone read the header
properly
would see it sure didn't come from the real xxxx.com. I've even had
TOSEmail
at AOL send complaints - aren't these guys meant to be experienced
admins?
Surely aol receives more than their fair share of spamming - these
people
should know what they're on about by now. I know places like
cybervalue.net
are having the same sort of problems.

matt

Denver airport baggage system simulations

luis fernandes <elf@ee.ryerson.ca>
Wed, 11 Dec 1996 17:21:02 -0500

The January 1997 issue of "Dr. Dobbs Journal" has an article in which
the
author reports that his software simulation of the automatic baggage
handling system of the Denver airport mimicked the real-life situation.

In his conclusion, he notes that the consultants did perform a similar simulation and had recommended against the installation of the system currently in place. The city, however, overruled the consultant's report (the contractors who were building the system never did see the report) and gave the go-ahead.

✈ A visit from the Goon Squad: computer evidence

+33)388412674 <"Nick BROWN" <Nick.BROWN@DCT.coe.fr> (Tel)>
11 Dec 1996 14:49:12 +0000

A field service engineer for a major computer company relates the following recent true story:

One day, he was working in a government office, when the police arrived with a search warrant. They asked, "which desk does Mr. X work at?". On being shown the desk, they proceeded to remove the Macintosh from the desk and took it away with them. Mr. X was not there to protest, having been incarcerated that morning on charges of forging identity papers using PageMaker, a Macintosh, and a high-quality color laser printer.

As the police left, everyone burst out laughing, not least at the thought that almost all the tools Mr. X was using (software and data files stored on the server downstairs, networked printer in the next-door office) were still sitting in the office. I don't know if anything incriminating was ever found on "his" Macintosh; perhaps he'll be found guilty of nothing more serious than possession of an unlicensed copy of AfterDark.

The RISKS? Well, apparently it's getting worthwhile (but not perfectly so !) to forge official documents at work, on company time, using taxpayer-funded high-quality printing tools; and secondly, of course, law

enforcement has a way to go in its understanding of how technology works,
but then I think we might already have suspected that.

Nick Brown, Strasbourg, France

🔥 Discussion of 'Computer errors' causes hernia (Minow, [RISKS-18.65](#))

Peter Ladkin <ladkin@TechFak.Uni-Bielefeld.DE>

Wed, 11 Dec 1996 20:42:15 +0100

In a piece entitled "Computer errors cause several plane crashes", Martin Minow summarised in [RISKS-18.65](#) an article from Aftonbladet suggesting the above. There ensued a lengthy discussion between Martin, myself, and Danny Kohn in Sweden, about the null-, whole-, or half-truth of most of the assertions. Of the 11 assertional sentences contained in Martin's quote, I found 10 of them misleading or false. Including, especially, the title. PGN suggested I *briefly* summarise the discussion. Faint hope.

I would argue:

- (a) against sensationalism and for precision;
- (b) against the common habit of picking on one of many contributory causal factors and calling it *the cause*;
- (c) for a classification of problems into computer-per-se/requirements/HCI;
- (d) against the assumption that even if computer behavior is directly causally involved, the *type* of error must be a computer error (I myself was disabused of this notion by Mary Shafer).

Martin would agree with me on (a) and (b), worries that the classification proposed in (c) may lead one to miss some important aspects of system failure, and is prepared to consider (d): he was struck by the similarity many of the (pre-heavy-automation) accidents discussed by Perrow ('Normal Accidents') bear to the (potentially computer-related) accidents we

discussed. Martin went to some trouble to distance himself from the views expressed in the article.

Martin would also like to point out that he has absolutely no training or competence in aircraft-safety and thus cannot judge the accuracy of the article, but definitely distances himself from the sensationalistic "death-trap" tone of the writing.

On the other hand, Danny thinks it is 'fully correct', and cites Reason's book on 'Human Error'. He considered some military aviation accidents, such as the two accidents with the Gripen fighter (I agree with the official position that these were control-system design problems, not computer problems per se). I also separate military aviation concerns from commercial aviation. Two cheers for diversity, I guess. But just in case the gentle reader doesn't believe in diversity, here's my view on journalistic sloppiness.

The Aftonbladet article suggested that new-technology airplanes are death-traps (the statistics actually show that they have a far better accident rate per departure than older-technology airplanes or even wide-bodies); claimed that 'technicians and engineers' are the people who test-fly the aircraft (patently absurd. In any case, pilots are very involved in the cockpit design of all new transports); and also seemed to be restricting its comments to the autopilot ("The critical point is when the computer system should be disconnected" - you'd hardly want to disconnect your control system, or your navigation information system, or your air data system, even were it to be possible).

The article apparently cited four accidents to justify its claim: AA, Cali 1995; Lauda Air, Thailand, 1991; Gottfro"ra (SE), 1990; Svalbard (SE) 1996. I consider these briefly. (Thanks to Martin for translations. He warns they're a little dog-eared, but I don't think this affects my points.)

Cali: "The accident investigation concluded that the contact between the pilot and computer system broke down [failed]."

None of the conclusions said any such thing. Readers may check the report for themselves in 'Computer-Related Incidents with Commercial Airplanes' at

<http://www.rvs.uni-bielefeld.de>

(This is not to deny the serious HCI issues that arose.)

Bangkok: "A computer error that caused one of the plane's engines to reverse could have caused the accident, concluded the investigation."

It is not possible for a 'computer error' alone to cause an in-flight thrust reverse on a B767. As I understand it, there is a hydraulic interlock which prevents this. It was determined in tests that there exists a failure mode of this interlock on high-time engines. No potential explanation other than (interlock failure *plus* pilot-uncommanded in-flight thrust-reverse request) has been found. No probable cause was determined.

Gottro"ra: "Both motors broke up. One of the better supported theories about the cause was problems in the computer system. The throttle [?] in one of the motors stopped working. The computer ran the other motor at full power and destroyed it completely."

It is my understanding that no probable cause was determined. Danny pointed out that this is a hot example amongst pilots in Sweden at the moment. However, I would caution against 'theory' which supposes computers are the modern form of gremlins. A synopsis of a PhD thesis on this accident may be found at

<http://info.admin.kth.se/info/pressmeddelanden/1995/0517-1.html>

This Swedish press-release was an invitation to Dr. Martensson's doctoral thesis defense.

Svalbard: "[...] a Russian passenger plane flew straight into a mountain [...] The accident cause is unclear, but there is a suspicion

that the computer system broke."

They said it themselves: the cause is unclear.

Does anyone actually know of *any* accident to a commercial airplane in which some sort of `computer error' is cited as the probable cause? Example and direct quotes, please. Caveat: `probable cause' and `contributing factor' are semi-technical terms.

Peter Ladkin

🔥 re: "Plane crashes" -- corrections ([RISKS-18.65](#))

Martin Minow <minow@apple.com>

Wed, 11 Dec 1996 21:47:57 -0800

There are two small errors that should be corrected in my item in [RISKS-18.65](#):

1. The correct URL for the Aftonbladet article is <http://www.aftonbladet.se/nyheter/dec/06/flyg.html> "aftonbladed" -> "aftonbladet" . As always, note that newspaper archives may not be kept for a long time.
2. The article title, "Computer errors cause several plane crashes" would be better translated as "computer errors a cause of several plane crashes." My translation made a sensationalistic Swedish article rather more sensationalistic than necessary.

There is an important "risk" here -- that technically sophisticated readers should avoid giving excessive weight to specific terms appearing in the popular press. Journalists often use "terms of art" without the precision and accuracy expected of scientific writing. In this case, readers must also understand that terms are translated from English to Swedish to popular-press Swedish and back to English, and have probably lost much of the subtlety and gradation of the original.

Martin Minow, minow@apple.com

✈ Re: Aviation Accident Rates (Kabay, [RISKS-18.63](#))

Peter Ladkin <ladkin@TechFak.Uni-Bielefeld.DE>

Wed, 27 Nov 1996 10:53:11 +0100

Mitch Kabay quotes Reuters quoting Michael Bagshaw, head of aviation medical services at British Airways, in an address to the Royal Society:

```
> "If we examine the accident rate by type of aircraft, it
> can be seen that although the overall trend is down ... new
> highly-automated types have a relatively higher accident rate."
```

Such statements need careful qualification. Boeing produces a statistical report on worldwide aviation accidents each year, from 1959-[present year].

My 1995 copy (courtesy of Pete Mellor) divides fatal accidents worldwide

into three classes: Second generation (B727, Trident, VC-10, BAC 111, DC9, B737-100/200, F28), Widebody (B747-100/200/300, DC10, L1011, A300),

and `New' (MD80/90, MD11, B737-300/400/500, B747-400, B757, B767, B777, A300-600, A310, A320/A321, A330, A340, BAe146, F100). The annual rate of fatal accidents per million departures since 1983 is in all years lower than that of either second-generation or widebodies, except for 1988, 1994 and 1995, when widebodies had 0 and new types non-zero rates.

The new types are all `glass cockpit' aircraft of the sort to which Dr. Bagshaw's comments are relevant.

So what can Dr. Bagshaw's comment as reported by Reuters be referring to? Maybe a different measurement. One that may seem *prima facie* reasonable is passenger deaths per passenger-mile. However, this measurement can be misleading, because 91.2% of fatal accidents occur in the takeoff or landing phases of flight, and only 8.2% in cruise. The widebodies spend most of their miles in cruise, and the new types are mostly short-haul aircraft which may only spend an hour to two hours in flight - similar to the second generation, whose accident statistics overall are worse. The different characteristics of airplane use could be reflected in the standard deviation: the figures, rounded to whole numbers, for widebodies from 85-95 are 1, 0,

1, 0, 3, 1, 2, 5, 1, 0, 0. Those for new types, rounded, are 0, 0, then all 1's. Those for second generation are 1, 1, 1, then higher than new's but less than 2, except for 94 (2). But these statistics do not reflect the vast differences in 'safety cultures' across the world's airlines. These differences can be large enough that the US prohibits aircraft operated by airlines in certain countries from flying into the US - and this system may be extended to Europe.

So, on these measures, the 'new technology' aircraft seem to be safer overall than other types. Dr. Bagshaw's measurements lead him to a different conclusion. The moral is: beware of facile quotation of statistics.

Dr. Bagshaw's comments on human factors are pertinent, and in fact justifiable independently of statistics. His comments focus on the cognitive capabilities of pilots, as 'information processors'. Such a view lies behind much current research in aviation human factors. And there have been some recent accidents which have focused attention on the pilot's awareness of the system state and its proper functioning: A320, Bangalore 1990; A320, Warsaw 1993; A300-600, Nagoya 1994; B757, Cali 1995; B757, Puerto Plata 1996. The reason for this attention is that these new systems allow failure modes (such as pilot's faulty awareness of system state) that simply didn't exist in older aircraft. Thus we need to pay attention to these problems and solve them, no matter what comparative accident rates are.

Solving such problems will, of course, affect accident rates, no matter how measured. Airline accident rates (pick your measure) are the lowest in history, but they do not appear to be going down. To bring this down,

it is reasonable to suppose that research and new techniques will be needed. And since nearly 60% of fatal accidents worldwide are primarily due to flightcrew behavior (Boeing again, 1985-95), human factors issues

must form a major part of this program. There are two aspects to this: establishing expectations of flight crew; and ensuring these expectations are met. The first is the focus of Dr. Bagshaw's comments: what can we reasonably expect from flight crew? The second is the business of appropriate and thorough training (that 'safety culture' again).

To summarise: it is appropriate, and appears to be necessary, to focus on human factors to reduce the rate of airline accidents (however measured). Recent accidents with 'new technology' have uncovered human factors issues that could not arise with older-generation aircraft. These new issues must therefore be addressed. However, I am

not aware that accident rates as currently measured and analysed enable us to judge whether 'new technology' aircraft are inherently 'safer' or 'less safe' than either second-generation or widebody aircraft (in Boeing's classification). They're 'differently safe'.

Peter Ladkin

✈ Re: Don't touch this switch! (Simpson, [RISKS-18.65](#))

Bear Giles <bear@indra.com>

Wed, 11 Dec 1996 19:57:54 -0700 (MST)

Why didn't the original sign state "Emergency Power Shutoff"? Who would casually press a button so labeled, especially in the offices of a "Major Computer Company."

Instead of being a bunch of dumb sheep, let's think about this situation.

(There's a lot of computer hardware and software which commits the same sin, after all.) _Why_ would "MCC" leave that switch in place, since it has obviously caused them much grief in the past?

The answer, of course, is it's an important piece of safety equipment. Computer rooms need emergency power shutoffs, and for those shutoffs to be useful in an emergency they can't be in the computer room itself. As I vaguely recall building codes won't even allow them in the doorway of the computer room; there has to be at least a doorway between the cutoff switch and the heavy electrical wiring.

Yet this important piece of safety equipment is effectively useless (and actually slightly harmful) since someone posted a paternalistic "do not touch" sign instead of posting a sign explaining the purpose of the switch.

It would be too much to suggest that we have a professional duty to press

every unlabeled red button we encounter, but the problem in this auditorium isn't the emergency power cutoff switch or the hard-to-find screen controls. It's the paternalistic author who thinks most people can't be trusted to know not to touch the cut-off switch if they know what it is -- and that they can't be trusted to know when it is important to use it.

Bear Giles bear@indra.com

🔥 Re: Don't touch this switch! (Simpson, [RISKS 18.65](#))

"Rosenthal, Harlan" <rosenthh@dialogic.com>
Thu, 12 Dec 1996 9:08:38 -0500

This is not a computer risk; it is the even more common human risk of people who seem to think that signs, lights, guide ropes, barricades, etc., apply to everyone but them. There is no way to design around such attitudes other than removing all potentially dangerous articles from their reach. Like child-proofing. :-)

-harlan

[As I have noted in the past, our forum deals with COMPUTER-RELATED RISKS (not coincidentally, the title of my book). Unfortunately, a lot of events that seem not to be computer risks are computer-related risks. When your computer wipes out, for whatever reason, that is certainly relevant here. People-tolerant systems is still a good research area. PGN]

🔥 4th ACM Conference on Computer and Communications Security

Mike Reiter <reiter@research.att.com>

Wed, 11 Dec 1996 17:02:13 -0500 (EST)

Fourth ACM Conference on Computer and Communications Security
(Preliminary Technical Program, Abridged for RISKS)
Zurich, Switzerland
1-4 April 1997
Sponsored by ACM SIGSAC

For more information, including registration and hotel information,
see: <http://www.zurich.ibm.ch/pub/Other/ACMsec/index.html> .

TUESDAY, 1 APRIL

4 half-day tutorials in two parallel tracks:

Theory Track

Practice Track

Morning	Cryptography Jim Massey, Ueli Maurer (ETH Zurich)	CERT and Practical Network Security Tom Longstaff (Software Engineering Institute)
---------	---	--

Afternoon	Internet Security Refik Molva (Eurecom)	Info-Wars Paul Karger (IBM TJ Watson)
-----------	---	---

WEDNESDAY, 2 APRIL

09:00-09:30 Introduction and Opening Comments
Richard Graveman (Bellcore)
Phil Janson (IBM Zurich Lab)
Li Gong (JavaSoft)
Clifford Neuman (Univ. of Southern California)

09:30-10:30 Invited talk 1: To Be Announced

10:30-11:00 Coffee Break

11:00-12:00 Session 1: Fair Exchange of Information

* Fair Exchange with a Semi-Trusted Third Party
Matthew Franklin, Mike Reiter (AT&T Research)

* Optimistic Protocols for Fair Exchange
N. Asokan, Matthias Schunter, Michael Waidner
(IBM Zurich Lab and Univ. Dortmund)

14:00-15:30 Session 2: Language and System Security

- * Static Typing with Dynamic Linking
Drew Dean (Princeton University)
- * Secure Digital Names
Scott Stornetta, Stuart Haber (Surety Technologies)
- * A Calculus for Cryptographic Protocols: The Spi Calculus
Martin Abadi, Andrew D. Gordon (DEC SRC and Cambridge)

16:00-17:30 Panel 1: Programming Languages as a Basis for Security
Chair: Drew Dean (Princeton), Panelists: To Be Announced

THURSDAY, 3 APRIL

09:00-10:30 Session 3: Authentication

- * Authentication via Keystroke Dynamics
Fabian Monrose, Avi Rubin (New York Univ. and Bellcore)
- * Path Independence for Authentication in Large-Scale Systems
Mike Reiter, Stuart Stubblebine (AT&T Research)
- * Proactive Password Checking with Decision Trees
Francesco Bergadano, Bruno Crispo, Giancarlo Ruffo (Univ. of Turin)

11:00-12:00 Invited talk 2: To Be Announced

14:00-15:30 Session 4: Signatures and Escrow

- * Verifiable Partial Key Escrow
Mihir Bellare, Shafi Goldwasser (UC San Diego and MIT)
- * New Blind Signatures Equivalent to Factorisation
David Pointcheval, Jacques Stern (ENS/DMI, France)
- * Proactive Public-Key and Signature Schemes
Markus Jakobsson, Stanislaw Jarecki, Amir Herzberg,
Hugo Krawczyk, Moti Yung (IBM TJ Watson and Bankers Trust)

15:30-16:00 Coffee Break

16:00-17:30 Panel 2: Persistence and Longevity of Digital Signatures
Chair: Gene Tsudik (USC/ISI), Panelists: To Be Announced

Banquet Dinner

FRIDAY, 4 APRIL

09:00-10:30 Session 6: Commerce and Commercial Security

- * A New On-Line Cash Check Scheme
Robert H. Deng, Yongfei Han, Albert B. Jeng,
Teow-Hin Ngair (National University of Singapore)
- * Conditional Purchase Orders
John Kelsey, Bruce Schneier (Counterpane Systems)
- * The Specification and Implementation of 'Commercial' Security
Requirements including Dynamic Segregation of Duties
Simon Foley (University College, Cork, Ireland)

11:00-12:30 Session 5: Cryptography

- * On the Importance of Securing Your Bins: The Garbage-Man-in-the-Middle Attack
Marc Joye, Jean-Jacques Quisquater (Univ. Louvain)
- * Improved Security Bounds for Pseudorandom Permutations
Jacques Patarin (Bull)
- * Asymmetric Fingerprinting for Larger Collusions
Birgit Pfitzmann, Michael Waidner (Univ. Hildesheim and IBM Zurich Lab)



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 18: Issue 67

Friday 13 December 1996

Contents

- [Washington State Unemployment Checks "Delayed"](#)
[Richard Berry](#)
- [More on the complexity of software upgrades](#)
[Nancy Leveson](#)
- [.pdf files -- RISKS of using Adobe Acrobat Reader](#)
[William Ehrich](#)
- [Re: Combatting cookies](#)
[Bruce Schneier](#)
- [Re: Amtrak ticket system breaks down](#)
[Robert Perillo](#)
- [Re: Aviation Accident Rates](#)
[Mark Stalzer](#)
- [Re: Don't touch this switch!](#)
[Darin Johnson](#)
- [Re: A visit from the Goon Squad: computer evidence](#)
[Scott Gregory](#)
- [CEPIS Statement: Security at risk due to encryption restrictions](#)
[Kai Rannenberg](#)
- [The InterNIC: a case study in bad database management](#)
[Jonathan I. Kamens](#)

[Info on RISKS \(comp.risks\)](#)

⚡ Computer malfunction causes panic selling at Hong Kong stock exchange

Joel Chan <joel@math.toronto.edu>

Fri, 13 Dec 1996 02:12:43 -0500

A computer glitch in the Hong Kong Stock Exchange caused panic selling on 12 Dec 1996 when its Teletext information system incorrectly reported a drop of 515 points (or about 4%) of the Hang Seng Index during the opening minutes of trading.

The error was blamed by a malfunction in the Automatic Order Matching and Execution System (AMS), which calculates up to the minute stock prices during trading hours. The Stock Exchange had apparently alerted dealers that there was a problem with the computer before trading began and were advised to use prices shown in free text areas for calculating opening quotations. However, the Teletext system made no indication of the computer glitch and instead displayed inaccurate stock prices until 20 minutes after trading began. The stock exchange is reviewing the incident.

Official figures for all indices and stock prices were finally released the evening after the exchange closed. The Hang Seng index, Hong Kong's main stock index, ended the day down 136 points (1.0%) at 13053.28. Volume was just over US\$1 billion. The loss was partly blamed by the computer glitch.

✂ Washington State Unemployment Checks "Delayed"

"Berry, Richard, Maj, AF/SCTA" <RBERRY@af.pentagon.mil>

Thu, 12 Dec 1996 14:20:03 -0500

>From the KOMO (Radio/Television station) news web site, 12 Dec 96:

"A state computer might be the Grinch that is stealing Christmas for some unemployed people. The computers cranked up two weeks ago to process claims for unemployment insurance have "mislaidd" checks for up to two-thousand jobless people. The weekly checks are as much as 365 dollars each. Employment Security commissioner Gary Moore notes that tens of thousands of checks were properly sent out. He says the system works well, but has some bugs that need to be worked out. But Moore also acknowledged that people who haven't gotten their checks need the money, and waiting for checks from the state is unacceptable."

✂ More on the complexity of software upgrades (Re: Bauer, [RISKS-18.65](#))

Nancy Leveson <leveson@cs.washington.edu>

Thu, 12 Dec 1996 18:19:54 PST

As an "old-timer" in this field (and an IBM systems engineer -- customer rep), we knew better than to assume that new software or hardware would work

correctly when first installed. It would be considered negligence to install something without running in parallel with the old system or installing it at anything but a low-activity time.

There are way too many untrained and ignorant people out there selling themselves as "consultants" or programmers. I've even had high school students tell me that they were hired to write safety-critical software. Is this their fault or the fault of people who think they can hire someone without training or proper credentials to do these jobs? I have never understood what it is about computers that that makes people believe that anyone can be an instant expert.

Nancy

⚡ .pdf files -- RISKS of using Adobe Acrobat Reader

William Ehrich <ehrich@minn.net>

Fri, 13 Dec 1996 08:20:11 -0600

A lot of the user manuals for Macintosh applications are now published using the .pdf format. They are expensive to print and hard to read on a monitor with less than 1800 x 2400 pixel resolution. So a lot of people don't read them.

Are there increased risks of various kinds from making user instructions less accessible?

- Bill Ehrich

✶ Re: Combatting cookies

Bruce Schneier <schneier@counterpane.com>

Fri, 13 Dec 1996 16:59:05 -0500

For a while I would have my Netscape browser alert me every time a cookie was sent, so I could refuse it. Some pages send three or more cookies upon loading, and this quickly became annoying. Recently I set up a batch file that trashes my cookie file every time I boot my computer up. Works great.

Bruce Schneier Counterpane Systems schneier@counterpane.com
<http://www.counterpane.com/> APPLIED CRYPTOGRAPHY

✶ Re: Amtrak ticket system breaks down ([RISKS-18.64](#))

<Perillo@DOCKMASTER.NCSC.MIL>

Thu, 12 Dec 96 16:01 EST

As reported in the New York Times, "Failure of Ticket Computer

Snarls Amtrak at Busy Time", Saturday 11/30/96, page 30. Amtrak's Central Computer did not go "belly up", but the communications/networking hardware that connects the ticketing

agents around the country to the Central Computer failed.

Starting about 12:30pm on Friday, Thanksgiving weekend, Amtrak's

reservation and ticketing system for the entire country broke down causing total chaos and long lines. As of late Friday

night

the system was still not working, But no train delays were reported.

Ticketing agents, dependent on the system and lacking printed tables of fares, in many cases guessed at fares and overcharged passengers.

While more information is needed, it seems strange that no Risk

Analysis was done prior to the breakdown to identify the piece of communications hardware as a possible single point failure (SPF)? Why wasn't a redundant communications link to the central computer available? This is standard Avoidance and Diversity (A&D) provisioning.

Plus, a manual backup system should have been in place. Ticketing agents should have had up-to-date printed tables of fares and forms, like the train conductors carry.

Robert Perillo, Perillo@dockmaster.ncsc.com

✉ Re: Aviation Accident Rates (Ladkin, [RISKS-18.66](#))

Mark Stalzer <stalzer@macaw.hrl.hac.com>

Thu, 12 Dec 1996 13:16:10 -0800

The trouble with the aviation accident statistics is that they only show that new airframe and engine designs with glass cockpits are safer than old airframe and engine designs with traditional controls. It could very well be the case that great improvements in the reliability of new airframes and engines are offsetting serious deficiencies in the modern controls. There is

a risk that manufacturers will hide behind the statistics and resist efforts to determine the dangers and benefits of high levels of cockpit automation.

Mark Stalzer, mas@acm.org

✶ Re: Don't touch this switch!

Darin Johnson <darin@connectnet1.connectnet.com>

12 Dec 1996 21:53:34 GMT

Speaking of not touching switches, I used to have a computer at work that had an odd button design. I don't want to say the name in public (Dell) though.

The power switch was big and easy to see and stuck out from the case. The reset switch was about the size of a pencil eraser, and flush with the case so that it could not be pushed with a finger. I had to use a pen cap to push the reset.

The only rational I could see is that they didn't want anyone pushing reset by accident, even though I managed to shut down power on it once by accident with my knee. Yes, pushing reset is bad (except that it's the number one solution given when you tell people that Windows isn't working right), but pushing the power button is worse. And that's exactly what's easiest to push, and if you stuck an average computer illiterate user in front of it, that's what they would push. Even those who noticed the reset button might

mistakenly assume that because of the deliberate design that it would be better to push power instead of reset (and maybe even start doing so on other systems with better button design).

Darin Johnson darin@connectnet.com

✉ Re: A visit from the Goon Squad: computer evidence

Scott Gregory <sgregory@inforamp.net>

Thu, 12 Dec 1996 20:00:51 -0500

The RISKS?

As Nick put it, the police in many countries have a long way to go in their understanding of computer crimes, however, just imagine what would have happened if the police had acted 'appropriately'. They would have impounded ALL servers in the building that Mr. X had a login to, or any that he might have been likely to have unauthorized access to. They might have taken ALL laser printers in the building. Or at least the one that was Mr. X's 'default' so that they could examine it. If Mr. X had access to other machines at the site, they would have taken those as well.

The RISK is more complex than first thought. The Jackson Games case in the U.S. was fought on similar grounds - what is fair seizure and what is not?

I imagine that the "major computer company" might have had 'major' problems had the police actually 'done their job'.

Scott Gregory - Mississauga, Canada.

✶ CEPIS Statement: security at risk due to encryption restrictions]

Kai Rannenber [<kara@telematik.iig.uni-freiburg.de>](mailto:kara@telematik.iig.uni-freiburg.de)

Tue, 26 Nov 1996 00:28:31 +0200

Council of European Professional Informatics Societies (CEPIS)
POLICY STATEMENT, 1996-October-20

Governmental Restrictions on Encryption Products Put Security at Risk

Worldwide, there is a political debate regarding the virtue or otherwise of a control of encryption, in particular whether the import, export, and production of cryptographic tools and their use should be restricted. In several countries legal regulations exist, in some others steps are undertaken towards such regulations. At present an OECD Committee is drafting guidelines on cryptographic policy.

But there are concerns; the Council of European Professional Informatics Societies (CEPIS) - with nearly 200,000 professionals in its 20 member societies, the largest European association of professionals working in information technology (IT) - has agreed the following statement:

Should one wish to employ electronic communication as the main vehicle for commercial and personal interaction, then one ought to be assured, and be

able to prove, that messages are

- not disclosed to unauthorised recipients (confidentiality),
- not tampered with (integrity),
- shown to be from the senders stated (authenticity).

It has always been an aim of secure reliable communication to comply with these requirements. The more the information society becomes a reality, the more enterprises, administrations and private persons urgently need the absolute assurance that these requirements are met.

To achieve this, so called "strong" cryptography is available. Several tools based on strong crypto-algorithms are in the public domain and offered on the Internet, others are integrated within commercial products.

A different technique for confidential and even unobservable communication is to use steganography, where secret data are hidden within larger inconspicuous everyday data in such a way that third parties are unable even to detect their existence. Hence there is no way of preventing unobservable secret communication.

To enable surveillance of electronic messaging, many criminal and national security investigators, i.e. police and secret services, demand access to keys used for encrypted communication. In order for this to be effective, escrowing (bonding) of these keys is advocated. However, for the reasons given above, key escrow (i.e. depositing copies of the keys with a "trusted third party", including back ups) cannot even guarantee effective monitoring. Moreover, key escrow already constitutes a risk for the secrecy of the keys

and therefore for the secrecy of the data. This risk is exacerbated in cases of central escrowing.

Besides, the burdens of cost and administrative effort as well as the loss of trust in communications could be significant and are prone to deter individuals and organisations, especially small business users, from gaining the benefits of modern information and communications systems.

Effective electronic surveillance of digital networks is difficult and time consuming, and requires extensive resources. In particular, closed groups such as criminal organisations might even use steganographic techniques to avoid any detection short of physical access to the terminals they use. Thus restrictions on encryption may be of very limited help in the fight against organised crime. On the other hand, the essential security of business and private communication may be seriously imperiled and economically hampered should they be subjected to insufficiently secured key escrow.

On these grounds, CEPIS recommends the following:

- (1) The use of cryptography for identifying data corruption or authenticating people/organisations should be free of restrictions and encouraged by governments.
- (2) All individuals and organisations in the private and public sectors should be able to store and transmit data to others, with confidentiality protection appropriate for their requirements, and should have ready access to the technology to achieve this.

(3) The opportunity for individuals or organisations in the private and public sectors to benefit from information systems should not be reduced by incommensurable measures considered necessary for the enforcement of law.

(4) The governments of the world should agree on a policy relating to their access to other people's computerised data, while seeking the best technical advice available in the world on:

(4.1) whether and which access mechanisms to computerised data are an effective, efficient and adequate way to fight (organised) crime and mount effective prosecution of criminals, and

(4.2) how to implement the policy whilst minimising the security risks to organisations and individual citizens.

(Evaluation and implementation of the policy will require regular review as the technology evolves).

Further Information:

Council of European Professional Informatics Societies (CEPIS)
7 Mansfield Mews
GB London W1M 9FJ
United Kingdom

Tel/fax: +44 171 637 5607
E-mail: cepis@bcs.org.uk
URL: <http://www.bcs.org.uk/cepis.htm>

The CEPIS Legal & Security Issues Network
URL: <http://www.wi.leidenuniv.nl/~verrynst/cepislsi.html>
E-mail: Kai Rannenberg (kara@iig.uni-freiburg.de), Secretary

✶ The InterNIC: a case study in bad database management

"Jonathan I. Kamens" <jik@cam.ov.com>

Thu, 12 Dec 1996 17:07:04 -0500

(This message was also sent to comp.protocols.dns.ops .)

The InterNIC (<http://www.internic.net>) is responsible for Internet domain name service for all top-level domains, as well as for second-level domains underneath all the old ARPA domains except MIL (EDU, GOV, NET, ORG, COM). Until a few years ago, domain registration services were provided by the InterNIC for free. That changed when they convinced the NSF that its grant money wasn't enough to cover their costs, so (amid much hubbub on the Net) they started charging \$50 per year for any second-level domain registration, with the first two years (i.e., \$100) payable in advance.

According to <<http://rs.internic.net/nic-support/nicnews/stats.html>>, the InterNIC registered 638,788 new domains between August 1993 and September 1996. If I'm doing my math right, at \$100 per domain, that's almost \$64 million, or over \$20 million per year. I would think that with that much money, they'd be able to provide competent service to their customers. Unfortunately, my experience has been that they're simply not doing an acceptable job. Some examples:

* Their automated systems do not function properly.

They've introduced a PGP-based system for authentication of domain contacts. In other words, they allow domain contacts to register their PGP public keys in the InterNIC public-key database, and then requests which come from those contacts will only be accepted as authentic if they are signed with the corresponding provide key.

Unfortunately, this system does not always work. Recently, I submitted a series of twelve database modification requests to the InterNIC in a single day. All of them were correctly signed with my PGP key. Of the twelve requests, three were returned to me in messages beginning, "We are not able to verify the PGP signed message that you sent us."

To make matters worse, for one of those three failed requests, I received a message claiming the the modifications I'd requested had been completed, two days *before* I received the message informing me that they were unable to verify my PGP signature.

I have asked the InterNIC multiple times why their system randomly fails to verify valid PGP signatures. They have not responded to my inquiries.

Interestingly enough, another poster to comp.protocols.dns.ops claimed that when he asked an InterNIC on the telephone about their PGP authentication system, he was told that it is not currently working. That would seem to indicate that the InterNIC is aware that there are problems with it, and yet they continue to advertise it on their Web site without any indication that it might not work for any given request.

* There are some data in the database which are impossible to update using the templates they provide.

One of the types of data stored in the InterNIC database is hosts; in particular, hosts which act as domain-name servers for domains registered with the InterNIC have records in the database.

Host records include an organization name and address associated with the host. And yet, the template for updating host records (available at <ftp://rs.internic.net/templates/host-template.txt>) does not have fields in it for updating that information! I believe that there are a couple of other record types in the database which have this same problem.

This organization/address data has been described to me by an InterNIC employee as an "old hold-over;" it seems that new host records do not have organization and address data, but old ones do. Nevertheless, one would think that when switching to a new format for host records, the InterNIC would have either removed the obsolete data from the old records or established a procedure for updating it.

Instead, the only way to update this information electronically is to send a plain-text message to hostmaster@internic.net explaining what you're trying to do, and then hope that whoever reads your message will be competent enough to understand what you're asking for and do the update by hand. Which brings me to my next point...

* When asked how to do something that is not handled automatically by their templates, their staff give incorrect answers (or simply ignore the query) more often than they give correct answers.

Of the twelve requests mentioned above, six of them were handled improperly by the InterNIC staff members who processed them. In several cases, I received a response instructing me to use a particular template to make the changes I had requested, when in fact those changes had nothing whatsoever to do with the template they told me to use.

I finally had to escalate my requests by sending "out-of-band" E-mail to an InterNIC employee who has resolved problems of this sort for me in the past, and she was able to "bounce" my requests to a high enough level that they actually got processed.

Incidentally, the InterNIC introduced one or more typographical errors into the data I sent them when processing six of my twelve requests (i.e., when they were done processing my requests, six of the twelve records I asked them to modify had one or more typographical errors in them).

I suppose that sending incorrect answers is better than how things were a few months ago -- then, if you sent a request that the person who read your message did not know how to answer, he/she simply ignored it and sent no response whatsoever.

* There are some data in their database which are impossible to update using

their current procedures.

Imagine this scenario... Joe Admin at Foo, Inc. is responsible for system administration, including DNS administration. He therefore has a contact record in the InterNIC database indicating that he works for Foo, Inc., and he is listed as a contact for various domain, network, and host records, in the InterNIC database.

Now, he leaves the company and takes a new job, with no further contact with Foo, Inc. He doesn't bother to update his contact record in the InterNIC database before he leaves.

Foo, Inc. would rather not let records remain in the InterNIC database claiming that Joe works for them when in fact he does not. Therefore, they want to contact the InterNIC and tell them, "Look, the information in Joe Admin's contact record which says that he for us is incorrect. You can confirm this by attempting to send E-mail to the address in the record, or by calling the phone number in the record and asking to speak to him. The person who answers will confirm that he no longer works there. Please either delete the contact record completely or remove the information in it which associates Joe Admin with Foo, Inc."

Sounds reasonable, right? Well, unfortunately, the InterNIC has *no procedures whatsoever* for allowing a company to remove contact information which incorrectly lists them.

I attempted to do just what I described, i.e., to get the

InterNIC to
remove the contact record for a former employee of OpenVision
who no longer
works here, and who I cannot contact to ask him to update his
own record
(and considering that it's not hurting him in any way, I don't
see that he'd
have any incentive to update it even if I could ask him to).

After several rounds of E-mail with the InterNIC, they called
me on the
telephone to discuss what I was trying to do. Once on the phone
with them,
I was "bounced up" through several layers of InterNIC staff,
until I was
finally able to speak to a woman who was perfectly willing to
admit that
yes, the scenario I described was a somewhat common one, and
yes, it was
perfectly reasonable for a company not to want the InterNIC
database to
associate non-employees with the company, but no, there's no way
for anyone
but the owner of a contact handle to update it. "Perhaps we
need to
establish a procedure for that, and I'll be glad to discuss that
for you
with our customer service manager, but we don't have one right
now," she
said, and she did not offer to make an exception and handle my
particular
request manually without the blessing of a "procedure".

Presumably, this means that I could edit my own contact handle
to
indicate that I work for any company that I want, and that
company
would have no way to get the InterNIC to remove the fraudulent
information.

Similarly, presumably, that means that (to be a little morbid
for a
moment), if someone listed in the InterNIC database dies,

there's no way for anyone else to get the InterNIC to remove the deceased's record from the database.

When I pressed the woman about this, she said to me, "If you're a network administrator at this company, you presumably have control over the mail server" (an assumption which is not always true, and indeed isn't true in this case; although I can ask the people who administer the mail server to make changes and hope that they'll listen, I don't have the ability to make the changes directly). "Well," she continued, "if you send us a mail message which claims to be from the former employee, asking for his record to be deleted, we'll process it."

"Let me get this straight," I responded. "You're telling me that I should forge E-mail to your system in order to delete this record." She confirmed that interpretation. I said, "Surely you see the absurdity of that."

She responded, "Well, obviously, ideally we wouldn't want anyone forging requests to our system, but in this case, that's the only way for you to delete the record."

"What if the former employee had associated a PGP key with his contact record before he left the company."

"Well, in that case, you'd need his private PGP key in order to delete the record."

"But surely you know that's impossible -- the whole point of

PGP is that only the owner a private key has access to it. Even if I had access to the file in which it was stored, I wouldn't know the correct password to unlock it."

"Well, in that case, there would be no way for you to delete the record."

There are a number of countries with strict laws about the collection of private information in computerized databases. Database maintainers are required to seek permission from all individuals who have data about them stored in the database, to guarantee the security of the database, and to establish working procedures for keeping the data in the databases up-to-date.

The United States has few such laws (there are laws about specific types of databases, such as credit and medical records, but no laws about databases in general). Until I started dealing with the InterNIC, I didn't see much point to them. Well, I've changed my mind. the InterNIC proves rather clearly that left to their own devices, companies will not maintain databases in a responsible manner.

Incidentally, nowhere on the InterNIC's WWW site can I find the address or telephone number of the governmental office which oversees their grant and handles complaints about their services. Several months ago, I sent them E-mail asking for them so that I could file a complaint, to be

considered

the next time their grant comes up for renewal. Like many of my other messages to them, that request was ignored.

Jonathan Kamens | OpenVision Technologies, Inc. | jik@cam.ov.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 18: Issue 68

Monday 16 December 1996

Contents

- [California tax-form attacks: a new tax on businesses](#)
[PGN](#)
- [Communications errors delay response to San Francisco fire](#)
[Brian Slesinsky](#)
- [Power surges in Third World countries](#)
[Frank Conlon via Don Wagner](#)
- [Re: repetitive strain injury suit](#)
[Joshua Goodman](#)
- [November, 1996 CACM article on InfoWar Defense - highly critical](#)
[Fred Cohen](#)
- [You can't rewrite history in Internet Explorer 3](#)
[Tim Nott](#)
- [*Java Security* by Gary McGraw and Edward W. Felten](#)
[PGN](#)
- [When is an upgrade not an upgrade?](#)
[Ian Barker](#)
- [Beware of Year2000 Sharks: A Story for Non-Believers](#)
[Year2000InfoNet](#)
- [Re: .pdf files, RISKS of using Adobe Acrobat Reader](#)
[Kenneth Albanowski](#)

[Gene Wirchenko](#)

● [Re: Combatting cookies](#)

[Hal Lewis](#)

[Frank Stuart](#)

[Pete Kaiser](#)

● [Women into Computing Conference 1997, last call for papers](#)

[Richard Nealon](#)

● [Privacy Digests](#)

[PGN](#)

● [Info on RISKS \(comp.risks\)](#)

⚡ California tax-form attacks: a new tax on businesses

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

Mon, 16 Dec 96 8:50:42 PST

A California Franchise Tax Board computer apparently went berserk, resulting in thousands of extra copies of 1996 tax forms being sent to California businesses -- including a San Diego dentist who reportedly received about 16,000 copies of the 1996 forms. [Source: An AP item in the *San Francisco Chronicle*, 14 Dec 1996, A16.]

⚡ Communications errors delay response to San Francisco fire

Brian Slesinsky <bslesins@hotmail.com>

Sat, 14 Dec 1996 17:22:19 -0800

>From Saturday's San Francisco Chronicle (Dec 14, page A20, also available online: <http://www.sfgate.com/wais/search/chron-pro.html>):

San Francisco fire officials acknowledged yesterday that communications errors delayed the arrival of vital equipment at last month's huge fire at Pier 48 -- the second time this year that the department has had problems getting firefighters to major blazes." [...] According to [Deputy Chief] Gamble, a dispatcher -- alerted to the waterfront fire at 2:48 p. m. -- initially sent only four pieces of equipment by computerized message when he should have sent seven. Gamble said the dispatcher mistakenly entered into the computer that the alarm had come from a street box, triggering a relatively minimal first response. The second error occurred when the first units at the scene immediately called for help. At that point, Gamble said, the dispatcher told the computer to send the next wave -- only to discover six minutes later that the units never got the message. Gamble explained that because the dispatcher gave the computer the wrong message on the first alarm, the computer wouldn't accept the second." [...]

The RISK seems to be a user interface that makes it too easy to make mistakes entering data, and "business rules" that assume that whatever was previously entered into the computer is correct.
Brian Slesinsky bslesins@hotmail.com <http://www.hotwired.com/staff/bslesins/>

Power surges in Third World countries

D B Wagner <106026.3213@compuserve.com>

Sat, 14 Dec 1996 06:13:14 -0500

Don Wagner, Reverdilsgade 3, 1.th., DK-1701 Copenhagen V DENMARK
[Don sent in another item too, but this one seemed appropriate
here. PGN]

>----- Forwarded Message -----

From: Frank Conlon, INTERNET:conlon@u.washington.edu
To: D B Wagner, 106026,3213
Date: Fri, Dec 13, 1996, 2:31

RE: H-ASIA: Using laptop in the PRC

Date: Thu, 12 Dec 1996 17:14:10 -0800
Reply-To: Frank Conlon <conlon@u.washington.edu>
Sender: H-Net list for Asian History and Culture <H-ASIA@h-net.
msu.edu>
From: Frank Conlon <conlon@u.washington.edu>
Subject: H-ASIA: Using laptop in the PRC
To: Multiple recipients of list H-ASIA <H-ASIA@h-net.msu.edu>

H-ASIA, December 12, 1996

Response to query on laptop usage in PRC from a non-Sinologist

>From Frank Conlon <conlon@u.washington.edu>

With reference to Susan Blum's query, I cannot say anything at
all about the
PRC, but will mention the strategy I followed whilst in India in
1990-91
using a laptop.

It may be too late or too unwieldy to use my approach, but what I
did was buy
several extra storage batteries and a charger. Except in Bombay
city which
had a relatively stable power system, I never, that is NEVER,
plugged my
computer directly into an electric source. During my previous
visit we had
purchased a top of the line, industrial strength surge protector

made in the
U.S.A. It lasted 6 days before the Delhi Electric Supply
Undertaking sent a
spike through the line and blew the little hummer into the next
world, if
there is a next world for surge protectors and transformers.

Instead, in 1990-91, since I had a computer that used batteries
which could
be replaced and charged in a separate charging device, I just
kept cycling
batteries through the charger and replacing them as needed.
Because I was
going to be there for almost a year, I purchased a substantial
surge
protector in India--the sort folks there buy for their
televisions and
refrigerators there. Being manufactured in India meant that
they were
engineered with a realistic grasp of the vagaries of most Indian
power
supplies. As the power surges came it buzzed and spat, but the
battery
charger blissfully escaped unscathed.

Now if you are travelling around a lot, that might be
inconvenient, and
perhaps such devices are not readily and cheaply available in
China, but my
computer and data reached home safely, and the surge protector
made a
handsome gift to one of the many folks who had done favors for
me during my
stay.

Bon voyage, bon chance.

Frank Conlon, University of Washington

✉ Re: repetitive strain injury suit (PGN, [RISKS-18.68](#))

Joshua Goodman <goodman@eecs.harvard.edu>

Fri, 13 Dec 1996 20:23:40 -0500

Repetitive Strain Injuries are a very common risk from computing; they can easily lead to disabling injuries. The fact that these people sustained million dollar injuries give you an idea of how bad it can be... However, RSIs can be avoided with proper typing technique, ergonomics, stretching, etc. For instance, simpler than installing foot-pedals is to train oneself to hit ctrl, shift, etc. with the index finger of the opposite hand. For tips about typing technique, and other information about RSIs, see <http://www.eecs.harvard.edu/RSI>, which is pretty good (OK, as the author I'm biased) although a bit Harvard specific. Another good page (OK, maybe better) is <http://www.engr.unl.edu/eeshop/rsi.html>.

🚩 November, 1996 CACM article on InfoWar Defense - highly critical

<fc@ca.sandia.gov>

Mon, 16 Dec 1996 09:42:54 -0800 (PST)

***** FLAME ON *****

Dateline: Livermore - Dec. 16 9:02AM

CACM AIMS RIGHT BUT MISSES INFO-WARFARE TARGET

Yes, Neil Munroe aimed right, but as usual, he missed the Info-Warfare target.

He correctly identifies the problem - disruption (a.k.a., corruption and denial of services) - but he misses the target by talking about privacy, privacy, and more privacy.

The phone system could be brought down... but we have to protect privacy

The power grid could go down... but we have to protect privacy

Planes could crash... but we have to protect privacy

Questions: Suppose we had absolute and perfect privacy but still had the current inadequate level of information assurance.

Could the phone system still be brought down? Yes

Could the power grid still be brought down? Yes

Could air traffic still be brought down? Yes

Does privacy protection solve the information assurance problem? NO!

Question: Suppose we had absolute and perfect information assurance.

Could we still have perfect privacy? Probably

So what is the relevance of the "... but we have to protect privacy" when the issue is not privacy but assurance (integrity and availability)?

If we aim at information assurance and we keep hitting privacy, we will never achieve our goal.

The target is NOT privacy!

This issue is NOT ABOUT PRIVACY!!

PRIVACY IS THE WRONG TARGET!!!

The right target is integrity and availability - a.k.a. information assurance.

How many times have I heard this misdirection? Hundreds at

least. What's the
cause? I don't know.

It could be that people think of computers as infallible and
that
for that reason integrity and availability cannot be of
concern.

It could be that people just don't understand.

It could be that the media attention and publicity is all
aimed
at privacy. I've even seen media stories of computer viruses
causing
computer crashes and heard the media people comment on how
privacy
problems have to be addressed in order to solve this.

Get a clue!

How come the editors at the ACM couldn't figure this one out and
tell the
author to hit the right target?

They must not have a clue!

How come the author calls the privacy advocates to find out about
information assurance?

He must not have a clue!

How come the FBI seems to think they need to tap phones to
protect NII
integrity?

They certainly don't have a clue!

How come the president puts people without a clue in charge?

The president doesn't have a clue either!

As clueless Louis once said:

"If you want to make sure your phone works,

make sure your number isn't in the yellow pages."

***** FLAME OFF *****

This article was sponsored by the "get a clue" foundation:
- people with clue trying to get it to you.

[Extensive disclaimers omitted.]

Fred Cohen can be reached at tel:510-294-2087 fax:510-294-1225

⚡ You can't rewrite history in Internet Explorer 3

Tim Nott <timn@cix.compulink.co.uk>

Mon, 16 Dec 96 14:02 GMT0

Microsoft Internet Explorer 3 for Windows 95 maintains two special folders. One, the 'Temporary Internet Files' folder, actually contains four MS-DOS directories, used to cache HTML documents, GIFs, JPEGs and other files downloaded from the Web. The other is the 'History' folder, which does a similar caching task, but for URLs. Although each URL appears as a separate entity in the folder they are actually stored in two .DAT files.

Clearing the History folder removes the entries visible in the Explorer folder, but does not delete, or reinitialise the DAT files. These are still visible using File Manager, and can be opened with a text editor to show all the 'deleted' URLs. The files cannot be deleted by normal means (including first resetting attributes) from within File Manager or Explorer. Presumably they are overwritten 'as needed' by new URLs. Risks? We know

where you've been today...

Tim Nott Figeac France

***Java Security* by Gary McGraw and Edward W. Felten**

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

Mon, 16 Dec 96 13:44:57 PST

Gary McGraw and Edward W. Felten

Java Security: Hostile Applets, Holes, and Antidotes --

What Every Netscape and Internet Explorer User Needs to Know

John Wiley & Sons, New York, New York, 1997

ISBN 0-471-17842-X

This book is mandatory reading for every user and developer of Webware.

It considerably extends what readers of RISKS have already learned,

and puts the entire topic into a coherent and readily accessible form.

***When is an upgrade not an upgrade?**

Ian Barker <ian@pumpptt.powernet.co.uk>

Mon, 16 Dec 1996 10:22:08 GMT

A few days ago a non-technical neighbour of mine asked me to pop over and

check out the new Pentium PC she had bought for her family and herself. She

is not particularly familiar with computers and this was her first PC. Her

main concern was that the computer dealer was going to "come back in a few

days" to upgrade the Pentium Chip from a 133Mhz to 166Mhz and

she wanted to make sure she wasn't wasting her time installing any new software if the upgrade was going to trash her hard disk.

The new machine was running Microsoft Windows '95 and the dealer had helpfully renamed the "My Computer" icon on the desktop to say "Pentium 133" - presumably as part of their standard installation process. Fair enough.

My neighbour told me the dealer had told her that the machine was "running at 95 percent full power" and that he would return in a few days to "switch it to 166Mhz". She *knew* it had 16MB of memory because the machine counted it as part of the boot-up process when the machine is switched on.

When the dealer's technical guy arrived (1 week later) he didn't have any parts or boards with him and he proceeded to rename the "My Computer" icon from "Pentium 133" to "Pentium 166". He fiddled around with the CD ROM (my neighbour had asked him to fix an unhealthy vibration). I hadn't told the technical guy that I was computer literate (I have my own software company) and he - wrongly - assumed that my neighbour's lack of knowledge was typical of all in the house.

The dealer's employee completed his inspection of the CD ROM and put on his coat ready to go. My neighbour's inquiries of "Is the PC running OK now?" were answered with assurances that all the work was completed and he was ready to leave - all this without once opening the PC case.

One assumes that either the dealer has been charging customers for Pentium 166 chipped PCs and installing the cheaper processors or the dealer's employee has been up to no good himself. Either way, my neighbour would have been no wiser - as far as she would have been able to tell the upgrade had been carried out as agreed. Technology is so advanced in her opinion that she thought it possible to upgrade the PC merely by sitting at the keyboard and typing. The processor inside the machine was actually a true Intel Pentium 133 (I checked!) but it could have been a Pentium 90, Cyrix or indeed just about anything else and a non-technical user would have had very little obvious way of checking.

The risks?

Just because a PC says it has a Pentium 133 inside it doesn't actually mean that it has. Just because someone says with authority that everything is as it should be it doesn't actually mean that it is. And always get a second opinion if you are about to spend a lot of money on something you don't really understand.

Needless to say my neighbour (and her rather large and incensed husband) took the PC back to the dealer and demanded her money back (which was finally paid by cheque even though she paid cash).

Ian Barker ian@pumptt.powernet.co.uk <http://users.powernet.co.uk/pumptt>

⚡ Beware of Year2000 Sharks: A Story for Non-Believers

Year2000InfoNet <mbsprog@idirect.com>

Sat, 14 Dec 1996 07:32:01 -0500

BEWARE OF YEAR2000 SHARKS: A STORY FOR NON-BELIEVERS

I offer the following story as a different slant on the effect Year2000 may have on companies. The Year2000 Shark may be after your customers too...

I was sitting in the waiting room of a tire-repair shop. The room was dingy, and the owner/manager behind the counter was covered in tire carbon from head to foot. Into this scene walked a well-dressed arrogant-looking fellow with a meek assistant. He walked up to the counter and assertively asked the manager if he knew whether his credit-card authorization system was Year2000-compliant. Needless to say, the manager was clueless.

The salesman offered to test the store's CC unit with a test card. No sooner had the manager given the slightest nod of agreement, the salesman was swiping his card through the unit and pointing triumphantly at the message that popped up saying the card was invalid. "This card," he said, "has an expiration date of January 30, 2000. This system is not Year2000-compliant. May I ask where you got this system and how much you paid for it..."

That manager was helplessly snowed by the circumstances. If there was some way for him to require that salesman to legitimize himself (and his test

card), it didn't occur to him. I thought about stepping in, but wanted to see where things went first. The manager succeeded in fending off the salesman's push for an immediate sale, so I figured he'd be OK.

THE MORAL: Even companies who have dealt with the Year2000 problem effectively need to ensure that their customers do not fall prey to such sharks or wily competitors who may seize the opportunity caused by the lack of information. I'm not a marketing person, but I imagine marketing staffs around the business world will be "strategizing" on this very soon, if they haven't already started...

The Year2000 Information Report thanks Jud Williford, Manager, Application Architectures/Technology Architecture Planning, Information Technology Division, Federal Express Corporation for submitting this article for publication. Jud can be reached at jlwillif@fedex.com, Tel: (901) 922-2349, Fax: (901) 397-4494. This article appears in the latest issue of the Year2000 Information Report.

mbsprog@idirect.com <http://web.idirect.com/~mbsprog> (416) 650-9475

✉ Re: .pdf files, RISKS of using Adobe Acrobat Reader (Ehrich, R-18.67)

Kenneth Albanowski <kjahds@kjahds.com>
Fri, 13 Dec 1996 21:21:06 -0500 (EST)

[It is] even harder to read on monitors with 80x8 pixel resolution, or 2x8 pixel resolution (Braille readers) or without a monitor at all (Speech synthesis). Not to mention simply difficult to read if your monitor doesn't match the aspect ratio of the original page.

As far as I can see, the risks are monumental. From my viewpoint, a format like HTML (which was designed to be accessible to everyone and every piece of software) is far, *_far_*, superior to a system which hands you dressed up photographs of each page in turn.

It may be simple for companies to produce .pdf documentation, but by doing so they sharply curtail the usefulness of the information.

Kenneth Albanowski (kjahds@kjahds.com, CIS: 70705,126)

✉ Re: .pdf files, RISKS of using Adobe Acrobat Reader (Ehrich, R-18.67)

Gene Wirchenko <genew@mindlink.bc.ca>

Sat, 14 Dec 1996 04:49:47 GMT

I'm sure glad I don't use a user-hostile system like a Mac. Instead, I use a user-hostile IBM compatible. My fun has been with Microsoft Visual FoxPro 5.0.

The Language Reference manual supposedly is a language reference manual, but it isn't. It has information on the syntax of the command, what the arguments are, BUT LITTLE TO NOTHING ABOUT THE SEMANTICS.

Fortunately, that is available in the on-line documentation. Needing a language reference manual, you might want to print all of the on-line docs. So you print it out. (Cost?) Then you find that the heading isn't printed. With most of the commands, the syntax diagram just down from the top has the item name, but with some retained for backward compatibility, they are only documented with something like "This feature retained for backward compatability. Use <something else> instead." and nothing else.

Did you want to print the topics more than one at a time? To do that, you put the topics you want into the on-line docs notepad (where they are listed in reverse order), print them (and find they print in reverse order (A nice match!)), and then delete them from the notepad (ONE at a time).

Are you finding this confusing? Try the on-line help for the on-line documentation. I got lost. It's the worst on-line help I've ever read.

The RISK? A customer (me) could refer to your manuals as "flingware" and raise hell with technical support. He might also switch to another product. (If the product itself wasn't reasonable, I might have.) VFP looks good, but if you can't get it going...

Gene Wirchenko

✶ Re: Combatting cookies (Schneier, [RISKS-18.67](#))

hal lewis <hlewis@physics.ucsb.edu>

Fri, 13 Dec 1996 19:51:01 -0800

I wish I knew why my solution---making the cookie file read-only---isn't just as good. Nobody ever writes to my cookie file, and nobody ever aborts a transmission (to my knowledge) just because they can't write to my cookie file. Am I missing something here?

Hal Lewis

[Also proposed by
Michael Schuerig <uzs90z@ibm.rhrz.uni-bonn.de> and
"Stirling Westrup" <sti@Hydro.CAM.ORG>. PGN]

✶ Re: Combatting cookies

Frank Stuart <fstuart@vetmed.auburn.edu>

Fri, 13 Dec 1996 23:14:33 -0600 (CST)

Making Netscape's cookies file a symbolic link to /dev/null is also an effective way to disable cookies under UNIX.

Frank Stuart fstuart@vetmed.auburn.edu

[Also proposed by
Brian Clapper <bmc@n2k.com> and
Rik Faith <faith@cs.unc.edu>.

A much more elaborate scheme was proposed by
Zygo Blaxell <zblaxell@myrus.com>,
replacing the set-cookie string with an equal-length random string.

Carl Maniscalco <caman@earthlink.net>
suggested a freeware utility called "Cookie Monster". PGN]

⚡ Re: Combatting cookies

<kaiser@acm.org>

Mon, 16 Dec 96 08:07:56 +0100

I also have "alert me" to cookies turned on in my Netscape browser, and last Friday I brought up a page that attempted to set twenty-nine cookies.

Anyone who does this to me is running a risk: the risk that I won't return to that page.

Incidentally, so far I've encountered nothing anywhere to make me permit a cookie.

Pete kaiser@acm.org

⚡ Women into Computing Conference 1997, last call for papers

Richard Nealon <Richard.Nealon@ITD.boi.ie>

Mon, 16 Dec 1996 13:45:47 +0000

WOMEN INTO COMPUTING CONFERENCE 1997 IN ASSOCIATION
WITH CENTRE FOR COMPUTING AND SOCIAL RESPONSIBILITY

To be held at De Montfort University, Milton Keynes, UK.
10th July - 12th July 1997

*** PAPER SUBMISSIONS DUE 6 January 1997 ***

PROGRESSION: FROM WHERE TO WHAT?

Computing and information technologies are now ubiquitous and of vital

importance in the global society. Gender related issues in computing continue to be critical in realising the potential of these technologies.

Computing as a discipline has a clear gender imbalance. Recent figures show recruitment of women into the discipline is continuing to decline.

To date, significant determinants of women's success in the computing field have been explored primarily in terms of societal, cultural and organisational work factors. The perspective of women computer technologists and engineers has often been overlooked. Tensions between the different groups exist but there has been insufficient dialogue between these different groups to date. This conference will address this situation and provide an opportunity for a greater understanding between all those working in and associated with computing.

Papers are invited within the broad area of Gender related computing research. This includes but is not limited to:-

1. Telematics -the field of computer mediated communication.
2. Women systems/software engineers - a contradiction in terms?
3. Professionalism, legislation and the role of women.
4. Women Returners
5. 'Man Machine' Interface to 'human Computer' Interface to what?
6. Feminist perspectives in computing research.
7. Education - computing education and the use of computers in education.

An underlying theme of the conference is to be social responsibility and therefore we wish to encourage papers emphasising this and ethical issues.

Papers taking different cultural, national and societal aspects are

particularly welcome as are globally oriented papers.

In addition, we are looking for sister organisations throughout Europe to participate in the conference. The aim is to report on European Women's Organisations, initiatives and relevant research. We will be maximising participation through the use of video conferencing services at De Montfort University.

For further details, or if you would like to register an intention to submit or participate in the conference, please email : wic97@dmu.ac.uk We will then add you to our mailing list for registration

Further information on Women into Computing can be found at:
<http://osiris.sund.ac.uk/wic/wic-home.htm>

Further information on the Centre for Computing and Social Responsibility can be found at:
<http://www.cms.dmu.ac.uk/CCSR>

Centre for Computing and Science, Social Responsibility e-mail: ccsr@dmu.ac.uk WWW : www.cms.dmu.ac.uk/CCSR/	Dept of Computer De Montfort University, The Gateway LEICESTER, UK LE1 9BH
--	---

Privacy Digests

"Peter G. Neumann" <neumann@csl.sri.com>
16 Dec 1996

Periodically I remind you of TWO useful digests related to privacy, both of which are siphoning off some of the material that would otherwise appear in

RISKS, but which should be read by those of you vitally interested in privacy problems. RISKS will continue to carry general discussions in which risks to privacy are a concern.

* The PRIVACY Forum is run by Lauren Weinstein, with some support from the ACM Committee on Computers and Public Policy. He manages it as a rather selectively moderated digest, somewhat akin to RISKS; it spans the full range of both technological and non-technological privacy-related issues (with an emphasis on the former). For information regarding the PRIVACY Forum, please send the exact line:

information privacy

as the first text in the BODY of a message to:

privacy-request@vortex.com

You will receive a response from an automated listserv system. To submit contributions, send to "privacy@vortex.com".

Information and materials relating to the PRIVACY Forum may also be obtained from the PRIVACY Forum Archive via ftp to "ftp.vortex.com", gopher at "gopher.vortex.com", and World Wide Web via: "<http://www.vortex.com>". Full keyword searching of the PRIVACY Forum Archive is available through the World Wide Web access address.

* The Computer PRIVACY Digest (CPD) (formerly the Telecom Privacy digest) is run by Leonard P. Levine. It is gatewayed to the USENET newsgroup comp.society.privacy. It is a relatively open (i.e., less tightly moderated)

forum, and was established to provide a forum for discussion on the effect of technology on privacy. All too often technology is way ahead of the law and society as it presents us with new devices and applications. Technology can enhance and detract from privacy. Submissions should go to comp-privacy@uwm.edu and administrative requests to comp-privacy-request@uwm.edu.

There is clearly much potential for overlap between the two digests, although contributions tend not to appear in both places. If you are very short of time and can scan only one, you might want to try the former. If you are interested in ongoing discussions, try the latter. Otherwise, it may well be appropriate for you to read both, depending on the strength of your interests and time available.

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 18: Issue 69

Thursday 19 December 1996

Contents

- [Bright Field crash in New Orleans computer related](#)
[PGN](#)
- [Bright Field: Risks of smart safety systems?](#)
[David Lesher](#)
- [Major denial-of-service attack on WebCom in San Francisco bay area](#)
[PGN](#)
- [Connecticut DPUC gets slammed](#)
[Daniel Pouzzner](#)
- [U.S. program export controls ruled unconstitutional in No. California](#)
[PGN](#)
- [German Cabinet Approves Internet Regulation](#)
[PGN](#)
- [More savings we can count on our fingers...](#)
[Jeffrey Sorensen](#)
- [URGENT! Major HOLE in NCSA httpd servers...](#)
[Matthew Healy](#)
- [Warning! Security risks with ActiveX!](#)
[B Fiero](#)
- [Re: November 1996 CACM article on InfoWar Defense](#)
[Geoff Kuenning](#)

- [Re: Software hunts and kills Net viruses](#)
[Gregory B. Sorkin](#)
 - [First Workshop on Building and Using CORBAsec ORBs \[urgent\]](#)
[Richard Soley](#)
 - [New Security Paradigms '97, call for papers](#)
[Yvo Desmedt](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✶ **Bright Field crash in New Orleans computer related**

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

Tue, 17 Dec 96 8:49:42 PST

According to John Hammerschmidt of the NTSB, preliminary investigations into the freighter *Bright Field* crashing into the Riverwalk in New Orleans suggest that an oil-pump failure caused the ship's computer to automatically reduce speed. A standby pump kicked in, but under reduced power the ship's maneuverability was decreased. The impact cut a 200-foot swath into shops and a hotel condominium complex, and the pedestrian walkway. A language barrier between the Chinese-speaking captain (and crew) and the English-speaking pilot reportedly may also have contributed. The Liberian-registered 69,000-ton ship was not equipped with a U.S.-recommended voice recorder, and a second voice recorder was not functioning. Coast Guard Captain Gordon Marsh confirmed that large ships lose steering power as often as once a week. [Source: various news items, including *San Francisco Chronicle*, 17 Dec 1996]

⚡ Bright Field: Risks of smart safety systems?

David Lesher <wb8foz@netcom.com>
Tue, 17 Dec 1996 07:50:00 -0800 (PST)

[... see previous item ...]

The pilot appears to have performed a miraculous job of parallel-parking the 761-foot vessel in the 900-foot space between two heavily populated entertainment boats.

The RISK? While [the automatic reactions] clearly saved an engine that likely costs millions to rebuild, could the sacrifice of the engine have prevented the collision? Or would have the engine exploded; throwing LARGE pieces around and killing people that way?

Is the low-speed version of the Airbus dilemma -- who knows more; the pilot or the computer?

⚡ Major denial-of-service attack on WebCom in San Francisco bay area

"Peter G. Neumann" <neumann@csl.sri.com>
Tue, 17 Dec 1996 08:56:06 -0500

A 200-message-per-second SYN-flood attack (see [RISKS-18.45](#) for the precursor PANIX attack, and [RISKS-18.48](#) for some defenses) was launched against WebCom (a large WWW service provider), affecting more than 3000 Web sites for 40 hours during most of what was otherwise a very busy shopping

weekend. The attack began Saturday morning PST shortly after midnight.

The initial attack triggered an automatic pager warning. WebCom engineers then traced the attack back to PSINet. Ten hours later PSINet traced it to MCI lines. MCI traced the attack route back to CANet, an ISP in Ontario, and then back to BC.Net. WebNet was unable to stanch the flood, so MCI finally blocked all traffic from CANet to WebCom -- allowing WebCom to restore service.

Apparently, WebCom had experienced a milder SYN attack the weekend before, so it was better prepared than it might have been otherwise.

[Source: High-Tech Attack Shuts Down Web Provider in Santa Cruz, an AP item written by but not attributed to Elizabeth Weise, seen in the *San Francisco Chronicle*, 17 Dec 1996, C18. PGN Stark Abstracting]

["Betty G. O'Hearn" <betty@infowar.com> submitted the entire AP item.]

✶ Connecticut DPUC gets slammed

Daniel Pouzzner <douzzner@mit.edu>
Tue, 17 Dec 1996 13:53:22 -0500 (EST)

In an amusing twist on the now-tired practice of slamming, Connecticut's Department of Public Utility Control (DPUC) had 6 of its 14 long-distance lines switched involuntarily from MCI to Wiltel. The story, run today (17 Dec) as a full-width headline on the front page of the Hartford

Courant,
quotes a DPUC employee: "They did WHAT???. Excuse me, we're the
DPUC, and we
got slammed?"

The change was orchestrated and confirmed by SNET, the local
telephone
monopoly; SNET also confirmed that Wiltel (owned by WorldCom, of
Jackson
Mississippi, and the fourth largest long distance carrier) had
sent a
request to SNET that the switchover be made.

The practice of slamming is so common that it behooves
regulators to
consider how the infrastructure might be altered to make the
practice
impossible. As a starting point, the hand-written signature of
the client
(or representative thereof) should be required for any change of
service,
but future systems will surely involve digital signatures which
are issued
on a per-call basis. As the line between packet-switched
networks and
pseudocircuit-switched networks continues to blur, a new type of
competition
will eventually come to the fore. In the future, we should
expect smart
telephones to automatically choose the cheapest route to a
destination.

In the meantime, with customers essentially at the mercy of
whimsical
telephony moguls, only two policies are viable: either avoid
becoming
a dialtone customer in the first place (avoiding both slamming,
and
outright theft of service by phone card and cell phone profile
trafficking rings), or be eternally vigilant.

-Daniel Pouzner Westport, CT

🔥 U.S. program export controls ruled unconstitutional in No. California

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

Thu, 19 Dec 96 8:42:45 PST

U.S. District Judge Marilyn Hall Patel has ruled in favor of Daniel Bernstein, whose Snuffle encryption program (and corresponding Unsnuffle for decryption) had been considered a munition under the ITAR regulations -- and therefore subject to export controls. She ruled that the government restrictions on the export of encryption programs are an unconstitutional interference with freedom of speech. However, the ruling does not extend to the constitutionality of the export controls themselves. Somewhat curiously, the ruling is not applicable outside of California's Northern District (e.g., Silicon Valley).

Earlier, dissemination of his research paper describing the algorithm had been blocked by the State Department in 1993. However, when that paper was deemed distributable abroad in 1995, the distribution of the software itself was still subject to export controls -- whereupon Bernstein sued. (See [RISKS-18.05.](#))

🔥 German Cabinet Approves Internet Regulation

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

Wed, 18 Dec 1996 03:34:31 -0500

German Chancellor Helmut Kohl's cabinet has approved a bill that seeks to protect Internet users' privacy and prevent smut and Nazi propaganda. The new law covers businesses such as telebanking and database services, as well as online services. Perhaps redundant, acts already prohibited in Germany such as conducting fraudulent business -- will also be illegal electronically. Responsibility for suspect content is on the ``suppliers'', not the service providers. The law requires the use of ``digital signatures''. It bans certain forms of tracking of individual usage, and encourages some anonymity. It also calls for descriptors that would permit automatic filtering of material unsuitable for minors. [Sort of a minor's lamp?] [Source: a Reuters item, by Terence Gallagher, 11 Dec 1996, via BEYOND THE FRINGE: vol 27 no 16, from: alm@znet.com, contributed in its entirety to RISKS by Betty O'Hearn, betty@infowar.com 813-367-7277. PGN Stark Abstracting.]

✶ More savings we can count on our fingers...

Jeffrey Sorensen <sorenj@alumni.rpi.edu>

Tue, 17 Dec 1996 10:54:03 -0500

Way back in [RISKS-13.40](#), I complained about New York's plan to install fingerprinting systems for welfare recipients. Back then the fraud was estimated to be between \$150 million and \$2 billion, give or

take 3 decimal
places.

I now live in Connecticut, and the 12 Dec 1996 New Haven Advocate reports that the Connecticut fingerprinting system (to catch welfare recipients "red-handed") cost \$5.1 million. The system has discovered six *possible* cases of fraud out of 70,000 recipients. That's \$850,000 each for people who receive \$300 a month.

Of course, the state maintains that the system has worked as a scarecrow and that an estimated 3,000 of the 7,000 people who never showed up to be fingerprinted probably never will. So there.

This isn't the first time that flimsy science is invoked in a hot-button political issue. Troubling questions remain:

- (1) Does the fingerprinting system work as intended, i.e. is it an accurate biometric device? How many are wrongly accused of being welfare cheats? How many cheats does the system miss?
- (2) How much fraud is there in the welfare system? Approximately?
- (3) In the absence of answers to 1 & 2, how do we judge if these systems are worth their price?
- (4) Is it appropriate to subject welfare recipients to this additional burden, or is it intended to demean and demoralize an already disadvantaged group?
- (5) Of those who are afraid, for whatever reason, to be fingerprinted, how many are being denied legitimate benefits?
- (6) Who in the political system cares about any of this?

If things continue this way, the states will probably blow their
block
grants on those new millimeter wavelength holographic imaging
scanners...

sorenj@alumni.rpi.edu

✶ URGENT! Major HOLE in NCSA httpd servers...

Matthew D. Healy <Matthew.Healy@yale.edu>

Wed, 18 Dec 1996 11:42:10 -0500

One of the utilities that comes with NCSA httpd -- a cgi program
called phf
-- has a serious security hole. With a suitable URL, it can be
tricked into
sending the /etc/passwd file to any user. A number of computers
here at
Yale School of Medicine have been compromised in this manner.

To check whether YOUR password file has been downloaded:

```
egrep 'phf' /etc/httpd.dir/logs/access_log | grep 'passwd'  
      ^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^ (or wherever your WWW  
server log is)
```

When I checked the logs on our WWW servers, I found that people
in several
different countries have recently downloaded /etc/passwd files.
So the bad
guys know about this one. Many bad guys know about this one.

IF YOU HAVE BEEN HIT BY THIS, then:

1. disable the phf script until you can install a version that
refuses
to display the password file
2. CHANGE YOUR PASSWORDS! When you do, choose passwords that
will resist

cracking with a dictionary. Remember that under most flavors of Unix

only the first 8 characters of a password matter, so a password like

apricot57tree is really just apricot5 to a cracker!

Matthew D. Healy Ph.D., Center for Medical Informatics, Yale School of Medicine

Matthew.Healy@yale.edu <http://paella.med.yale.edu/~healy>

⚡ Warning! Security risks with ActiveX!

BFiero CT <bfieroct@aol.com>

17 Dec 1996 04:46:04 GMT

With Java, there was a sort of `Java virus' scare. Remember, anyone? It ended up being an application that put a load on your processor. It was real tough to hit that Back or Stop button in Netscape to stop the application, and then not go to that site anymore. Java programmers were quick to point out that the Java language can't access your operating system at all, much less do any damage.

But with Microsoft's Active-X, there are many more serious concerns. A programmer can access your memory and disk i/o sub-systems using Microsoft's Active-X. What does that mean? Well, ... the easiest thing a malicious person would do is plant a virus quietly on your system, or simply delete important files. But I believe Gates' plan is to be able to extract more information from your system. What? Forget so soon that when you electronically register Win95, your directory tree structure and

other
information is sent to M.\$ with your registration info?

This a quote from `Computerworld'. December 2, 1996 Vol. 30 No.49
On page 139 you'll find ...

*_*_*_*_Quote Begin

FIX ACTIVE-X SECURITY PROBLEMS. Objects built with ActiveX can
access system
resources on users' desktops, which can lead to security
breaches or
corruption of PC data. Microsoft's answer is to provide
certification the
ActiveX code comes from the developer that users think it comes
from. But
that isn't good enough, said Oliver Pflug, president of
SiteCast. Users must
"set up software to receive certificates, understand the entire
process and
have a way of verifying the certificate," he said. "It's
awkward."

*_*_*_*_Quote End

Is this what you want when using the Internet? To have to worry
about
properly setting up software to prevent people from taking
advantage of
M.S.'s intentional security flaws? And even then, this doesn't
prevent a
`certified' content provider from accessing data from your
system.

At Comdex it was finally made public knowledge that Billyboy
plans on
creating a `Microsoft Java.' Why? Because as hard as Microsoft
tried, it
couldn't take over and control the development of the real Java.
So now
instead of supporting something that would be a good thing,
Gates wants to
use strong-arm tactics to wipe out something that works well and

replace it
with his versions and `visions' of how he feels it should be. Of
course,
people are hard at work making M.S. Java incompatible with what
is out there
now. And code is already being worked on that will enable M.S.
Java to be
able to extract information from your system while you use the
Web, just as
ActiveX does now.

It's bad enough that Microsoft can retrieve stuff from your hard
drive, but
here's one thing I really fear ... As you may know, web pages
are stored on
your hard disk in a cache as you view them. Frequently accessed
sites can be
retrieved from there and displayed more quickly. But say someone
writes some
Active-X or M.S. Java code to randomly grab a couple of those
cache files
while you view their web page? Let's say they get one where you
entered your
credit card # to order that rare Pink Floyd album from a record
dealer on
the web. Or possibly a file on your disk that contains sensitive
personal or
business information?

All I can say is... Be afraid of using M.S. products, be very
afraid.

**✉ Re: November 1996 CACM article on InfoWar Defense (Cohen,
[RISKS-18.68](#))**

Geoff Kuenning <geoff@ficus.cs.ucla.edu>
18 Dec 1996 00:21:34 GMT

I am quite surprised that our esteemed moderator allowed Mr.

Cohen's rather
excitable, accusatory, and low-content article to be published
as it
appeared. Peter must have been having a busy day, or perhaps
this was the
cleaned-up version. [Geoff, You are kind. But I try not to be
a draconian
censor -- only a moderator. Besides, it triggered *your*
response. PGN]

In any case, I fear that it is Mr. Cohen who misses the point.
The issue is
not one of cluelessness, it's one of priorities. Mr. Cohen asks:

> Questions: Suppose we had absolute and perfect privacy but
still had the
> current inadequate level of information assurance.

>
> Could the phone system still be brought down? Yes
> Could the power grid still be brought down? Yes
> Could air traffic still be brought down? Yes
> Does privacy protection solve the information assurance
problem? NO!

>
> Question: Suppose we had absolute and perfect information
assurance.

>
> Could we still have perfect privacy? Probably

The point Mr. Cohen misses is that for some of us, privacy is
vastly more
important than information assurance. I'm not willing to accept
his
"probably." So all I have to do is turn his questions around,
replacing all
of his yesses with "probably" or even just "maybe," note that we
could then
have perfect privacy, and for me the decision is preferable.
It's hardly an
accident that the Founding Fathers of the United States chose to
make law
enforcement more difficult than it has to be.

Some of us (e.g., many FBI employees) place security above liberty. Others prefer the reverse choice. In neither case does that reflect on the quality of our reasoning.

Mr. Cohen is not clueless, but neither am I. I am, however, trying to be somewhat more polite.

Geoff Kuenning g.kuenning@ieee.org geoff@ITcorp.com
<http://fmg-www.cs.ucla.edu/geoff/>

✶ Re: Software hunts and kills Net viruses (Rosbach, [RISKS-18.65](#))

"Gregory B. Sorkin" <sorkin@watson.ibm.com>
Tue, 17 Dec 96 14:05:11 -0500

[RISKS-18.65](#) contains an item "Software hunts and kills Net viruses" (Hans A. Rosbach) that refers to a London **Times** article of the same title. (The **Sunday Times**, 1 Dec 1996, Innovations: Bits & Bytes.) Curiously, the same section of the Times includes articles entitled "Skull pins keep wigs in place" and "Cheeseburgers are rich in cancer-fighting compounds". (See <http://www.sunday-times.co.uk/news/pages/sti/96/12/01/stiinnbit01003.html?1483095>.)

Despite the fact that the article quotes me by name, as far as I know I was not interviewed by the **London Times**, and certainly the article gives an inaccurate account of IBM AntiVirus.

It is true that IBM AntiVirus contains a neural network which

detects new viruses by generalizing from old ones. It is also true that we are building towards an "immune system for cyberspace", whose functions will include an automated analysis of any new virus detected on a machine, and transmission of the results --- notably a procedure for removing the virus --- to affiliated machines. The prototype software is undergoing extensive testing, and will not be released until we are confident of its reliability.

We would of course never design a program to spread to any system whose owner hadn't explicitly arranged for it to be there, nor do we have any release scheduled for this week.

For those interested in the technical details, let me also mention that temporal difference learning has nothing to do with the neural network in IBM AntiVirus. Temporal difference learning was used for the very powerful backgammon-playing neural network developed by Gerry Tesauro, and Gerry also helped develop the anti-viral neural net, but there is no other connection between the backgammon network and the anti-viral one.

For more information about computer viruses in general and IBM AntiVirus in particular, please see <http://www.av.ibm.com/>

Gregory Sorkin, IBM T.J. Watson Research Center, 30 Saw Mill River Road
Hawthorne NY 10532 <sorkin@watson.ibm.com>

✶ First Workshop on Building and Using CORBAsec ORBs

[urgent]

Richard Mark Soley <soley@omg.org>

Wed, 18 Dec 1996 17:06:10 -0500

To Persons Interested in Security in Distributed Object Systems, the deadline for workshop participation is 20 Dec 1996.

FIRST WORKSHOP ON BUILDING AND USING CORBASEC ORBS
Marriott Inner Harbor, Baltimore, MD 21201, 1-3 April 1997
Co-Sponsored by the Object Management Group and the National Security Agency

The Object Management Group (OMG) CORBA specification includes security protocols and services that are being widely adopted. Unfortunately, a full understanding of the strengths and weaknesses of the security aspects of the CORBA standards requires experience with Object Oriented Technology, Information Technology Security and operational system planning, development and deployment. OMG is hosting this workshop to bring together individuals with varying sets of these types of experience to examine, explain and critique the adopted OMG security specifications and other similar and related work.

The workshop approach will be to have individuals with the full range of OOT, IT Security, and Operational System experience examine and discuss, in turn, the content and meaning of the CORBA Security standards, the design issues relevant to realizing the CORBA Security standards in ORBs, and the design issues relevant to using ORBs meeting the CORBA Security standards as the foundation for operational systems.

Interested individuals or organizations are invited to submit a brief position statement of one printed page (or 60 80-character email lines of text) outlining a position on one or more of the three major categories [CORBA security standards, Secure ORB design issues, Secure ORB usage issues] by 20 December 1996 to secws-submissions@omg.org . [Contact Richard Soley or David Chizmadia immediately for detailed information. I did not find it on the omg.org webpage. PGN]

WORKSHOP COMMITTEE Co-Chairs:

Dr. Richard Soley
Vice President & Technical Director
Computer Research
Object Management Group
soley@omg.org

Mr. David Chizmadia
Office of INFOSEC

National Security Agency
dmc@tycho.ncsc.mil

✦ New Security Paradigms '97, call for papers

"Dr. Yvo Desmedt" <desmedt@blatz.cs.uwm.edu>
Thu, 19 Dec 1996 00:09:12 -0600

PRELIMINARY CALL FOR PAPERS NEW SECURITY PARADIGMS '97

A workshop sponsored by ACM and the University of Newcastle upon Tyne.

Langdale Hotel, Great Langdale, Cumbria, UK
23 - 26 September 1997

Paradigm shifts disrupt the status quo, destroy outdated ideas, and open the way to new possibilities. This workshop explores deficiencies of current computer security paradigms and examines radical new models

which address those deficiencies. Previous years' workshops have identified problematic aspects of traditional security paradigms and explored a variety of possible alternatives. Participants have discussed alternative models for access control, intrusion detection; new definitions of security, privacy, secrecy and trust; biological and economic models of security; multiple policies; and a wide variety of other topics. The 1997 workshop will strike a balance between building on the foundations laid in past years and exploring in new directions.

[This is an important workshop, but attendance is limited to about 25 people. Somewhat surprisingly, the committee folks in the full notice total 23, but I suppose that they are not all going to attend. To participate, please get from Mary Ellen Zurko or Catherine Meadows the full information regarding your submitted paper, justification for your would-be invitation, and your commitment to attend all three days, which must be received by 4 April 1997. PGN]

E-mail to: newparadigms97@opengroup.org
use anonymous FTP from: <ftp.cs.uwm.edu>
in directory: [/pub/new-paradigms](ftp://ftp.cs.uwm.edu/pub/new-paradigms)
Use World Wide Web from: <http://www.cs.uwm.edu/~new-paradigms>

NEW SECURITY PARADIGMS '97 WORKSHOP ORGANIZERS

Steering Committee: Tom Haigh, Bob Blakley, Mary Ellen Zurko, Catherine Meadows, John Dobson, Hilary Hosmer

Workshop Co-Chair: Tom Haigh, voice: +1 (612) 628-2738,
fax : +1 (612) 628-2701, email: Haigh@sctc.com

post : Tom Haigh, Secure Computing Corp., 2678 Long Lake Road
Roseville, MN 55113 USA

Workshop Co-Chair: Bob Blakley, voice: +1 (512) 838-8133

fax : +1 (512) 838-0156, email: blakley@vnet.ibm.com

post : Bob Blakley, IBM, 11400 Burnet Road, Mail Stop 9134
Austin, TX 78758 USA

Program Committee Co-Chair: Mary Ellen Zurko, voice: +1 (617)
621-7231

fax : +1 (617) 621-8696, email: zurko@osf.org

post : Mary Ellen Zurko, The Open Group Research Institute
11 Cambridge Center, Cambridge, MA 02142 USA

Program Committee Co-Chair: Catherine Meadows, voice: +1 (202)
767-3490

fax : +1 (202) 404-7942, email: Meadows@itd.nrl.navy.mil

post : Catherine Meadows, Naval Research Laboratory Code 5543
Washington, DC 20375 USA



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 18: Issue 70

Friday 20 December 1996

Contents

- [BART software crash and system delays](#)
[PGN](#)
- [Problems of "unforeseen" system aging](#)
[Nick Brown](#)
- [LAPD Database Flaws in L.A. Weekly](#)
[Jeremy Leader](#)
- [The Risks of Security](#)
[Robert J. Perillo](#)
- [ATM gangsters](#)
[Andrew Weir](#)
- [Justice Wants to scrutinize Parolee computer use](#)
[Pete O McVay](#)
- [SATAN Survey](#)
[Christopher Klaus](#)
- [PCs and configuration management](#)
[Jeremy J Epstein](#)
- [Arrogance of Micro\\$loth Products - BEWARE!](#)
[Roland Giersig](#)
- [Re: Cookies](#)
[Mark J Cox](#)

- [More on the phf bug in NCSA httpd...](#)
[Matthew Healy](#)
 - [9th annual FIRST conference: Call for Papers](#)
[Stephen E. Hansen](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✂ BART software crash and system delays

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

Fri, 20 Dec 96 9:56:52 PST

Bay Area Rapid Transit (BART) had another bad day. At 7am, a ghost train appeared at the San Francisco 24th Street station, requiring manual operation through that station. Independently, three trains had to be taken out of service because of mechanical problems. All of this caused a 15-minute delay systemwide. Later, a computer crash caused delays up to 30 minutes systemwide, from 5:50pm to 9:45pm on 19 Dec 1996.

BART also had a serious power cable outage in the transbay tunnel on 12 Dec 1996 (not previously reported here by itself, because of its lesser relevance to the computer systems -- although it certainly had a major effect on the system as a whole). That cable problem was traced to sloppy maintenance after the cable was damaged way back when it was installed back in the early 1970s. BART now observes that an overall cable overhaul had been considered prior to the 12 Dec outage as an urgent step in upgrading the aging infrastructure.

✶ Problems of "unforeseen" system aging

+33)388412674 <"Nick BROWN " <Nick.BROWN@DCT.coe.fr> (Tel>
20 Dec 1996 09:55:44 +0000

Reading some back issues of RISKS, I realised how many of the incidents and problems reported are due to systems (embedded and otherwise) getting old. The "system" (made up of the people who use it, as well as all the computer "systems") has to be able to cope with the oldest and newest technology in it, and all the breakdowns in all the (non-upgradable) component systems. With the pace of change in technology (try buying a 1 megabyte SIMM), we are going to find ourselves more and more unable to maintain the systems we build.

Current examples are such things as: air-traffic-control computers being kept going long after the manufacturer can officially no longer supply the spares, by wizened (i.e., over-45) hardware engineers with soldering irons and a bag of those big fat 20-watt resistors; car "computers" which tell you the car's average speed over the last hour, for the first four years of the car's life, and then flash "88 8888" at you unless you spend \$1250 for a replacement unit; a four-year-old PC for which you can't buy a new disk drive (the BIOS can't handle anything bigger than 512 MB).

Future examples: anything with a smart card in it; the often-documented problem of reading information stored on 30-year-"guaranteed"-

lifetime

optical disks in 30 years when the disk might be readable, but no computer system can connect to the drive; and of course the year 2000.

People are very good at adapting to change (once they get over the emotional hurdle of accepting it's going to happen) and working with the limitations of old and new; just look at any home with items as diverse as a TV and a toilet. Computer systems aren't at all good at it, and anything with firmware is just disastrous.

Here's a little test for readers who work in systems specification. Have you ever seen a requirements, functional, or design specification for any computer application system that specified not just the hoped-for start date for production use of the system (you know, the one where you have to subtract a year for political reasons, even though you know there's no way it'll be ready in time), but also the END date, after which the system would be taken out of use and replaced with something else? For advanced students: what would have been the effect on any given project of doing so?

Nick Brown, Strasbourg, France

[The juxtaposition of this item with the BART item is of course purely coincidental(!). PGN]

LAPD Database Flaws in L.A. Weekly

Jeremy Leader <jeremy@worlds.net>

Fri, 20 Dec 1996 13:00:39 -0800

This week's L.A. Weekly (Vol. 19, No. 4, page 15) has a story about inaccuracies in the Los Angeles Police Department's Police Arrest and Crime Management Information System (PACMIS).

The following is my summary of some RISKY aspects of the story.

The article focuses on a doughnut shop in Van Nuys. Because the shop is the closest establishment to the street in a mini-mall, many incidents nearby bear its address in police records. That may be useful for getting officers to the scene quickly, but it resulted in the shop being described as a "disorderly establishment" because of the number of crimes recorded at its address, the majority of which had no connection with the doughnut shop.

The article paints PACMIS records as being very inaccurate. The examples cited include multiple entries for the same incident, and an entry that described a nearby jay-walking citation as a "felony prostitution" arrest on the premises of the doughnut shop.

PACMIS is not intended to be used for "evidentiary purposes", but the story claims PACMIS reports are used to influence zoning board hearings and other nuisance-abatement measures.

The story doesn't describe what PACMIS's original purpose was.

It sounds to me like a typical instance of the risks of inaccurate data and of using data for other purposes than those for which it was collected.

Jeremy Leader, Tujunga, CA, USA

✶ The Risks of Security

<Perillo@DOCKMASTER.NCSC.MIL>

Thu, 19 Dec 96 16:41 EST

The Superintendent of the Palisades Park, NJ, school system had to explain to the School Board an \$875 bill from a 16-year-old "hacker" who was hired to break into the schools computer system. The 19 Aug 1996 meeting was reported by the AP, and was carried by most national newspapers, such as the **Richmond Times-Dispatch**, 22 Aug 1996, "Hacker frees transcripts", page A16.

It seems that some students or former students, whose plans had changed, desperately needed transcripts sent off over the summer. The computer and database containing the students' records were locked via passwords, and no one who knew the passwords could be reached. The principal and former vice principal were on vacation and unreachable. The school employee who had the codes was recently incapacitated by a stroke. Members of the guidance department were furloughed for the summer because of the school's budget crunch and could not be found.

The school's computer coordinator asked the 16-year-old "computer whiz" to break into the system, and unlock the files so the various transcripts could

be printed. He did, and billed the school system \$25 an hour for 35 hours of work.

I believe this story shows the Risks of security, password access, and encryption systems, and the need for built-in "Key Recovery" architectures. Businesses and other organizations cannot be put at Risk, when critical information cannot be unlocked because of an employees absence, incapacitation, or lost keys and passwords.

Companies like AccessData, Orem, UT, do quite a lot of business in terms of password recovery for unlocking files. Unfortunately, these techniques, or the techniques used by the "hacker" would not be effective in systems using modern security and cryptography.

"Key Recovery" or "Key Archival" has long been recognized as a necessary function and service of security and cryptographic systems. While it is true, that in the U.S., a Court could order that one of the archived keys/passwords be released to the court, there are legal and procedural safeguards in place. There are far greater risks, such as losing the key/password, and having critical information lost and undecipherable. In the case above, the future livelihoods and careers of the students who immediately needed their transcripts would have been put at risk if they were unable to unlock the passwords.

Robert J. Perillo, CCP
mil

Perillo@dockmaster.ncsc.

[Reminder: RISKS readers will undoubtedly be able to make the

distinction

between "key recovery" for stored data and "key recovery/archive/escrow/

or-whatever" for communications. The situations are quite different.

RISKS readers will of course also be familiar with the potential risks

inherent in the presence of any mechanism that allows key recovery by an

untrustworthy third party. PGN]

ATM gangsters

Andrew Weir <100637.616@CompuServe.COM>

20 Dec 96 15:13:17 EST

Much British media panic has been devoted to the recent conviction of an "ATM gang" of high ambition. A collection of high-grade villains with impeccable pedigrees in robbery, gangsterism and drugs dealing over 30 years compelled a software expert who was in prison for attacking his wife and child to help them in their enterprise. The man revealed his role to a prison chaplain and subsequently acted as an undercover informer on his release.

The plot was to tap telephone lines carrying encrypted ATM card details to and from the banks, especially the Visa and Access (Mastercard's name in the UK) centres in Essex. Having decrypted the information, fake ATM cards with genuine cardholders' details would be manufactured from the 140,000 blanks they had bought. Teams of associates armed with the cards would then assault

thousands of ATMs in the UK and abroad.

The media response, based on the claims of the prosecution, said the plot had "put the entire banking system in danger". Not only that, but prosecution estimates of the potential proceeds were put at about L800 million, with chief counsel adding that in fact, "the sky was the limit".

The claims of the prosecution were alarmist, even if the conspirators were in deadly earnest, and bear the hallmarks of media fantasies about the true level of risk in bank security (see suspicions about the Sunday Times reporting on this in [RISKS-18.17](#)). The logistics alone of the planned ATM raids would have been horrendous. It would have been extremely difficult for a "raider" to use more than one ATM card after another at one machine without raising immediate suspicions. Typically, ATM cards have withdrawal limits no higher than L200 in the UK, often much lower, depending on the status of the account.

If one imagined that one person could cover, say, 50 machines in a -- very busy -- day and got L200 from each machine, he would clear L10,000 in one day. If, say, 100 gang members could withdraw that much each per day (a generous estimate), it would take them 160 days of continuous raiding to reach the prosecution figure of L800 million. It seems highly probable that within a short time of the raids beginning, alarm bells would go off throughout the banking system and ATMs would either be closed down, put under surveillance, or new, lower limits on all cards imposed by

the banks. (There would be loss of a public confidence in ATMs, but hardly a collapse of the banking system). Security cannot be good in a gang that big, and the chances of one of them being caught and spilling the beans, especially after the tremendous hue and cry that would have gone up, would have been very high.

Code-breaking gangsters?

But could they have got that far? Newspaper reports failed to emphasise the all-important question as to whether the encrypted information could be decoded. Defence counsel were scathing about the possibilities and called experts to testify that it was effectively impossible. One of the defence barristers said: "The basic method was fatally flawed ... because the encryption system used by the banks is so secure that no current technology available in the world, not even the combined expertise of the world's leading scientists, is capable of breaking it."

The judge appeared to accept this, with a proviso. Addressing the defendants, he said in sentencing them: "It was not possible for you, with the equipment and expertise then at your disposal, to carry out this fraud to a successful conclusion. There is, in particular, no evidence that the cards recovered by the police would then work or that the codes had then been broken. However, beyond that I'm not prepared to go. I do not believe it is necessary to go further but for the avoidance of doubt I make it clear that it would, in my judgment, be irresponsible and wrong on the

basis of
the information before me to accept any additional assurances
along the
lines that this is a fraud that no one could ever commit."

Lawyers being what they are, the judge could not exclude the
possibility
that the decryption was possible, even though the remoteness of
that
possibility does not seem to have struck home, particularly when
it is
considered that the gang's only computer expert was working
against
them. The gang's expert claimed no expertise in cryptography and
yet said in
evidence that there had been a successful decryption dry run.
This was not
corroborated elsewhere, and the judge did not accept it.

The case in court did not, as a result, measure up to the
headlines. In
fact, the prosecution had decided from the start only to charge
the men with
conspiracy to steal, which carries a maximum sentence of seven
years,
instead of conspiracy to defraud, which carries a maximum of 14
years. For
the latter charge to succeed, the Crown would have had to
convince the jury
that the defendants had "a reasonable chance of success".
Despite the gang
spending some L100,000 in the purchase of equipment, making
numerous
clandestine visits to British Telecom telephone exchanges, and
suborning
about three BT engineers, the prosecution realised such a charge
would fail.

The judge kept his head and, in the end, the ringleader was
sentenced to
only five years in prison, some subordinates to four and three
years, and
the man whose heavily guarded country home was the headquarters

for the plot
only got a two-year suspended sentence. It is worth remembering
that
sentences reflect the convicted person's criminal record, and
the "form" of
these men was awesome.

Computerised fraud on a gigantic scale has been a major focus of
media panic
and large-scale exaggeration in the past. The criminal
community, it seems,
was guilty of believing everything it read in the papers.

Justice Wants to scrutinize Parolee computer use

Pete O McVay <pmcvay@world.std.com>

Fri, 20 Dec 1996 13:14:18 -0500

In a copyrighted story dated December 19th, Rex Nutting of
TechWire reports
that the U.S. Justice Department is considering new rules to
restrict access
of Federal Parolees to computers and the internet.

Restrictions being considered include "requiring parolees to
keep a daily
record of their computer use, requiring parolees to agree to
unannounced
inspections of their computers, banning the use of private or
public
computer networks without prior permission and banning the
possession or use
of data encryption programs."

Lawyers and law enforcement experts termed the new rules "silly"
and
"unenforceable". Regardless of these opinions, I attach a more
sinister
meaning to this proposal. The U.S. Justice Department is
reinforcing a

prevalent government attitude that private citizens use the internet primarily for criminal purposes.

For some reason, it is all right for large corporations or organizations to surf the net, and also to use encryption to protect their data and financial transactions. But the Justice Department rules imply that private citizens doing the same thing must have something to hide, or are searching for illegal materials--bombs, pornography, electronic vandalism methods, etc.

To my knowledge, parolees are not required to report visits to their local libraries, where much of the same information can also be found. Perhaps we need laws that require that borderline institutions such as libraries not be located in high-crime areas or near prisons...

SATAN Survey

Christopher Klaus <cklaus@iss.net>
Fri, 20 Dec 1996 09:03:40 -0500 (EST)

Here's some extremely alarming information made available by Dan Farmer. It has a good break down of sampled sites that were assessed and what the number of them were vulnerable or misconfigured.

I'm sure these sites probably didn't use SATAN (<http://www.fish.com>) or ISS (<http://www.iss.net>) to secure themselves. 8-

The survey is available at <http://www.trouble.org/survey>

P.S. In light of security experts conducting these surveys, I'd recommend using tools like RealSecure and Courtney to detect when you unknowingly become a statistic in these surveys.

... I guess it is accepted practice to scan at will as long as you do not break in?

cklaus@iss.net Christopher William Klaus, Internet Security Systems, Inc.,
Ste. 660, 41 Perimeter Center East, Atlanta, GA 30346 (770)395-0150

PCs and configuration management

JEREMY J EPSTEIN <JEPSTEIN@cordant.com>

Fri, 20 Dec 1996 09:07:16 -0500

It's no secret that PC hardware manufacturers modify machines continuously without changing model numbers, thus making it very hard for end users to maintain consistent configurations. These changes are usually swapping one model of peripheral for another or one brand of chip for another, and less commonly changing board layouts. These changes are done to reduce manufacturing cost, improve reliability, and/or deal with parts availability.

According to the December 1996 edition of Byte (pg 28), at least one large PC vendor recently made an incompatible BIOS change without changing the BIOS revision label displayed at boot time. The problem was discovered

because one machine ran Windows NT, while an ostensibly identical machine wouldn't. The RISKS of poor configuration management, driven by the industry drive for reduced cost and increased performance, claim another victim.

[As an aside, software vendors have taken to making changes without changing the version number also, in a process known as a "blind update". JJE]

[It is the next step in the process after the "blind date". PGN]

⚡ Arrogance of Micro\$loth Products - BEWARE!

Roland Giersig <roland.giersig@aut.alcatel.at>

Tue, 10 Dec 1996 11:37:30 +0100

This is about a "feature" in WinWord 6 that a colleague stumbled across. The incident shows the full arrogance that MS products exhibit when dealing with situations with ambiguous semantics.

The said colleagues job was to prepare monthly reports about estimated and real work-power efforts regarding some projects work-packages. For the first few months he wrote these reports using the WinWord installed on his laptop. Recently he switched over to using the WinWord installed on a central NT server using WinCenter to access it remotely from his Sun workstation. As it is common practise with such recurring reports, he opened

the report from last month to change the figures and save it under a new name.

Now the figures were listed in a table, and the sum of each column was calculated via the "Table Formula Sum(above)" function. Before he started changing the numbers, he accidentally pushed F9 ("Update Fields") while the cursor happened to be in the sum field.

Can you imagine how big his surprise was when suddenly the column sum CHANGED before his eyes? Remember, he didn't change anything! And WITHOUT WARNING! And to add insult to injury, the sum was WRONG!

Avid MS "fans" surely know by now what was wrong: the LANGUAGE settings of the two Windows versions differed! And thus the symbol for the decimal point was `.` on the one machine and `,' on the other.

The arrogance? NO WARNING! And the sum function does not even just truncate then numbers, no, it somehow interprets the comma or period as a list, because summing "1,4" and "2,3" gives... TADAH! "10"!!! (it used to give "3,7" with the other language settings)

The RISK? I really wonder how many reports are out there with wrong numbers because some poor dilbert-type employee typed it on his computer and her boss printed it from another computer with different language settings. Maybe even someone got degraded or fired "because s/he reported the wrong numbers"!

Also, WinWord is the only editor I know where you open a file, close it

again and WinWord asks you if you want to save the changes!!

(Another example of built-in arrogance: I tried to import some ASCII-text records into MS Access. Instead of asking about the format, Access silently tried to interpret the text itself and finally reported "1746 errors found"!)

So the final lesson learned is:

>>> MS documents ARE NOT PORTABLE! <<

(And another example of non-portability: MS Project stores the workdays-per-week number as a PER-USER setting, not per-project! Exchange a Project with a colleague and BINGO! Everything gets re-scheduled.)

There are surely lots of other examples, maybe others would like to share their "experiences" too.

BTW, I am sure that some of these "features" are or will get fixed. But I am also sure that nobody will receive a bugfix or upgrade for free, as it is common practise with other software companies. Instead you will be prompted to "upgrade to Windows97 and WinOffice2000 for a real cheap \$999.99 now and your problems will be solved". Sweet arrogance!

My feelings are best reflected by this signature found on the Net:

"Microsoft is not the ANSWER.
Microsoft is the QUESTION,
and the ANSWER is NO!"

Roland

PS: Sorry if this sounds very emotional, but I have already

wasted
enough precious time with things like these.

Roland.Giersig@aut.alcatel.at (speaking only to, err, for
myself)
ALCATEL Austria, Scheydgasse 41, A-1210 WIEN. Phone: +43-1-
27722-3755

✶ Re: Cookies (Stuart, [RISKS-18.68](#))

Mark J Cox <mark@ukweb.com>
Fri, 20 Dec 1996 16:04:14 +0000 (GMT)

> Making Netscape's cookies file a symbolic link to /dev/null is
also an
> effective way to disable cookies under UNIX.

There's been a lot of talk recently about disabling Cookie logs
in Netscape
- theres a simpler (undocumented?) way of doing this you might
want to
mention in a future journal.

In the Netscape preferences file there is an option
"ACCEPT_COOKIE" that
gets set to "0" if you want to always accept them, and "1" to
prompt the
user for every new cookie. Setting it to "2" doesn't prompt the
user and in
fact disables cookies altogether.

Mark Cox, Technical Director, UK Web ----- [http://www.ukweb.com/
~mark/](http://www.ukweb.com/~mark/)
Latest news on the Apache Web Server ----- [http://www.
apacheweek.com/](http://www.apacheweek.com/)

✶ More on the phf bug in NCSA httpd...

Matthew D. Healy <Matthew.Healy@yale.edu>

Thu, 19 Dec 1996 19:58:18 -0500

I got e-mail from `_many_` people pointing out:

- o this bug in phf and other sample CGI programs that come with the NCSA httpd distribution has been known since March 1996.
- o it allows many other tricks in addition to grabbing the `/etc/passwd` file. If you have one of the buggy CGI programs installed, then intruders can use it to do essentially anything that can be done by whatever userid your httpd server runs under.

The degree of tact ranged from courteous to downright rude.

Some people

implied that I must be a grossly incompetent webmaster not to have fixed

this one months ago. But this is an academic research facility, not the CIA

-- and even the CIA website did get cracked, though I don't know which hole

was exploited in their case!

I do try to keep up, but I am not a full-time security

specialist; I do many

different things, and I'm usually behind on most of them. After two weeks

wasted cleaning-up after the crackers, I am even farther behind than usual.

So, it seems to me that there are lessons to be learned from

this episode on

several levels:

- o I personally am more conscious of security issues than I was before

- this attack. I will spend more time keeping up with security alerts

- that might affect my site, and I will add scanning my

webserver log for

suspicious URLs to my list of things to check on a daily basis. Of

course, this will mean less time for my real work, and this does anger

me. Even a supposedly-harmless intrusion requires a responsible

administrator to spend untold hours checking for damage, looking for

backdoors and Trojan horses the intruders might have left behind, etc.,

etc. The cracker left a note claiming we had nothing to worry about

because he didn't damage anything, but in fact he did do a small

amount of damage without apparent malicious intent. And he did a large

amount of damage to my confidence in the integrity of my systems!

o Steps are being taken on an institution-wide level here at Yale to

improve the channels for coordinating responses to things like this.

When the wizards began checking other Yale servers for this hole, they

discovered that our servers in the Medical school are not the only

recent victims of phf attacks.

o Perhaps the Internet-wide channels for propagating alerts need to be

refined. I believe part of the reason I missed this hole was the sheer

number of alerts coming from various quarters that I and other

overworked system administrators are expected to read. It is simply not

reasonable to expect that every system administrator will apply every

recommended security patch every time yet another patch is released!

There needs to exist a mechanism for prioritizing warnings

according to

the ratio of severity to ease-of-exploiting each threat.

The phf hole

is so nasty precisely because anyone who is reasonably familiar with

Unix can learn to exploit it in a matter of minutes. And many crackers

are exploiting this one right now.

Matthew.Healy@yale.edu <http://paella.med.yale.edu/~healy>

9th annual FIRST conference: Call for Papers

"Stephen E. Hansen" <hansen@stanford.edu>

Thu, 19 Dec 1996 11:11:50 -0800

C A L L F O R P A P E R S

The Forum of Incident Response and Security Teams (FIRST)
Ninth Annual Computer Security Incident Handling Workshop

"Bridging the Borders - Incident Handling in an International Network"

Marriott Hotel, Bristol, England

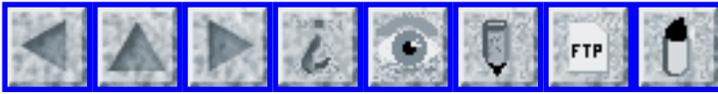
Monday 23-Jun-1997 to Friday 27-Jun-1997 (inclusive)

Abstract Submission Deadline: 15-Jan-1997. The complete call for papers

can be found at <http://www.first.org/workshops/1997/cfp.html> .

Contact Information: first-prog97@first.org for e-mail,
FAX: +1 415 725 9121 (Attention to: Stephen Hansen, Subject: FIRST 1997, Wkshp)

or or via post, Attn: Stephen Hansen, 333 Sweet Hall, Stanford University,
Stanford, CA, 94305-3090 USA



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 18: Issue 71

Monday 23 December 1996

Contents

- [Ghost 911 calls: software upgrade brings police](#)
[Timothy L. Kay](#)
- [Re: Ghosts](#)
[PGN](#)
- [Bright Field accident in New Orleans](#)
[Michael Quinlan](#)
- [ACTION ALERT: Stop the spread of personal information on the net](#)
[Jon Handler](#)
- ["Cryptography Policy and the Information Economy" draft available](#)
[Matt Blaze](#)
- [Security vulnerability in CERN access protection](#)
[Christopher Fraser](#)
- [Re: Emergency Key Recovery and Reconstruction](#)
[Adam Shostack](#)
[Bill Murray](#)
- [Protean documents](#)
[Daniel P. B. Smith](#)
- [Re: Problems of "unforeseen" system aging](#)
[Andrew Koenig](#)
[Paul E. Bennett](#)

- [Re: PCs and configuration management](#)
[Henry G. Baker](#)
 - [Microsoft documents and Rosetta stones](#)
[Darrin B. Jewell](#)
 - [Re: Arrogance of Micro\\$loth Products](#)
[Bob Vaughan](#)
[Jonathan I. Kamens](#)
 - [Secure passwords on the web? Not at Microsoft!](#)
[Andrew Marc Greene](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✂ Ghost 911 calls: software upgrade brings police

"Timothy L. Kay" <timkay@wacko.org>
21 Dec 1996 18:11:59 GMT

I use software that sends pages by dialing my modem and communicating directly with the paging company's paging terminals. I was using first-generation software that didn't understand area codes, so I had to enter the full dial string, 1-408-xxx-xxxx of the paging terminal. It worked fine.

Then I downloaded a new version of the software, which is much more "intelligent" about area codes and dialing. It now expects the user to enter numbers without the leading 1, such as 408-xxx-xxxx. (I didn't know this.) If the number matches your area code, it strips the area code. Otherwise, it adds a 1 before the number. The new software also defaults to a PBX configuration in which you have to dial 9 to get an outside line. (I didn't know this.)

I tried my first page. The software compared my area code (415) with the prefix of the number it was to dial (1-408-xxx-xxxx). It found that 415 does not match 140, and therefore prepended a leading 1. It also prepended a 9 to get an outside line. The software then dialed

9-1-1-408-xxx-xxxx

The police showed up about 5 minutes later. They confirmed my phone number and asked why I didn't answer their return call. I replied that it is my modem number, and I thought somebody was sending me a fax.

I have reported this problem to the software manufacturer, and I assume they will address the problem. In their case, upgrades to their software lead directly to the problem I described. (The tech support person replied that my description probably explains "something else that was happening.")

Bad design aside, a simple practice should be observed whenever software dials the phone: the software should have a sanity check to make sure that 911 isn't being dialed. For that matter, wouldn't it make sense for modem manufacturers to include such a sanity check in their modem firmware? Are there legitimate reasons for a modem to dial 911?

Tim

[Yes, but also Yes. PGN]

✉ Re: Ghosts ([RISKS-18.70](#))

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

Mon, 23 Dec 1996 8:15:24 PST

Well, Timothy gives us another example of ghost phone calls.

Long-time

RISKS readers will recall

* [RISKS-2.27](#): Ghost phone calls to 911 from cordless phone interference

when batteries ran down

* [RISKS-16.88](#): Calling Number ID ghost calls (from preprogrammed demo

model?)

In response to my BART ghost-train item in [RISKS-18.70](#), a RISKS reader asks,

WHAT IS A GHOST TRAIN? Answer: A train that isn't there but that the

computer believes IS there. Here are a few from the RISKS archives:

- * SF Muni Metro: Ghost Train recurs, forcing manual operation
- * SF Muni Metro: Ghost Train reappears; BART problems same day
- * Chunnel has ghost trains, emergency stops (due to salt water?)
- * `TCAS Sees Ghosts' (see IEEE SPECTRUM, August 1991, p.58)
- * Chicago's O'Hare Airport radar lost planes, created ghosts

It all ghost to show, especially if you are in the show.

Bright Field accident in New Orleans

Michael Quinlan <mikeq@primenet.com>

Sat, 21 Dec 1996 22:45:08 GMT

[Surprised?]

``The captain also acknowledged forgetting he had a computer

override

button on his console that could have allowed him to bypass the computer

and increase the ship's speed and maneuverability.''

Michael A. Quinlan mikeq@primenet.com <http://www.primenet.com/~mikeq>

⚡ ACTION ALERT: Stop the spread of personal information on the net

Jon Handler <jhandler@ils.nwu.edu>

Mon, 23 Dec 1996 10:52:55 CST

By permitting individuals to publish information about themselves and their activities, the Internet has become a powerful tool for creating new social connections across the barriers of geography and background. Recently, though, several firms have started abusing the power of the Internet to publish large databases of personal information without permission. This is impolite, and in many cases it can even be dangerous.

True story: recently, I followed a lead from MacUser magazine to a web page for dealing with spam e-mailers. That page suggested that one of the first steps to take was to contact services that track people's e-mail addresses. With growing horror, I connected to page after page on the list and located myself in their databases. Some services listed far more than just name and e-mail address. My home address and phone number were accessible from the same record. Two services even had a facility to show a

map of my neighborhood and the location of my house in it.

The widespread dispersal of information of this sort, without prior consent, is a serious invasion of privacy. In some cases, publishing personal information can be harmful to the individual. For example, battered women have very good reasons to keep present addresses confidential. Because these services gather their data silently, from many sources, they present a real threat to those who require anonymity. In addition, public databases serve as a source for stalkers, scam artists, and junk mailers. Because they potentially support these activities, databases of personal information weaken the social environment of all people on the net inhabit.

Below I have listed the URL's for the pages, along with the information that they contain and the contact address for that site. Send mail to the contact address, requesting that they 1) remove you from their database and 2) refrain from including you in the future. Note, the mail you send must contain enough information for the services to know which record to delete. It's best to send the information that the service tracks. Also, be aware that, unfortunately, there is no legal obligation for the companies to remove your name.

<http://www.four11.com>

e-mail/phone

support@four11.com

<http://www.whowhere.com>

e-mail/phone/address

delete-entry@whowhere.com

<http://www.switchboard.com>

e-mail/phone/address

webmaster@switchboard.com (DELETE in the subject line)

<http://bigfoot.com>

e-mail/phone/address/map

overexposure@bigfoot.com

<http://www.searchamerica.com>

This service requires a subscription to view information.

Their information page claims that they track names, addresses, and telephone numbers.

webmaster@searchamerica.com

<http://www.abii.com/lookupusa/adp/peopsrch.htm>

phone/address/map

consumerupdate@abii.com

Jon Handler jhandler@ils.nwu.edu

✶ "Cryptography Policy and the Information Economy" draft available

Matt Blaze <mab@research.att.com>

Fri, 20 Dec 1996 18:59:06 -0500

RISKS readers may be interested in a draft of my critique of US crypto policy. It summarizes comments I made to a recent meeting of the Computer and Communications Industry Association, and is an updated version of testimony I gave to the Senate Commerce Committee earlier this year.

Postscript is at <ftp://ftp.research.att.com/dist/mab/policy.ps>
ASCII text is at <ftp://ftp.research.att.com/dist/mab/policy.txt>

-matt

✦ Security vulnerability in CERN access protection

"Christopher Fraser" <chrisf@suede.sw.oz.au>

Sun, 22 Dec 1996 15:53:26 -0500

Some time ago I came across a security vulnerability in the access protection code in CERN httpd. I reported it to CERN last February but I haven't received any reply and the bug is still in the current sources. The bug is interesting because because it highlights a general risk which may be present in other Internet software.

CERN accepts access protection as either IP address patterns (such as 192.14.203.*) or as DNS hostname patterns (*.softway.com.au). Because the two share a similar syntax it uses the same code to the comparisons. However, it's entirely possible to construct DNS names that look like IP addresses and match the access protection rules. (I did a quick survey and the only other net software I could find which has the same problem is INN).

The bottom line is that if you run a the CERN httpd server as a proxy on a gateway machine and you use IP address patterns to restrict access to the proxy, external attackers can use the proxied services to access internal machines. This vulnerability exists even if your site filters out IP source address spoofed packets and has a paranoid resolver library.

I can supply a rough patch to interested parties; please contact me if you would be prepared to test it. Otherwise, a patch will be available from

<http://softway.com.au/misc/cern.html> in the next few days. In the meanwhile, if you are currently using CERN as a proxy on a gateway machine, I would highly recommend using router or host OS IP filtering to restrict access to the proxy service. Additionally you may want to look at newer proxy software, such as Squid, which may or may not be more secure (I haven't looked).

Christopher Fraser chrisf@sw.oz.au

[Re: Emergency Key Recovery and Reconstruction \(Perillo, RISKS-18.70\)](#)

Adam Shostack <adam@homeport.org>
Mon, 23 Dec 1996 09:57:30 -0500 (EST)

Robert J. Perillo writes of a school that hired a teenager to break in, and points (properly) to the need for key recovery mechanisms for encryption systems. There is, of course, a risk when a backup system is created.

The principal and former vice principal were on vacation. (Shouldn't the passwords have been changed?) Another employee had a stroke. So, who present should have been able to authorize emergency key release if the files had been encrypted? The recovery system probably should have a wide notification feature, to help detect misuse, but whom to notify, and would they understand the messages they receive?

✈ Re: Emergency Key Recovery and Reconstruction (Perillo, [RISKS-18.70](#))

"William Murray" <whmurray@dtus.com>

Sat, 21 Dec 1996 20:50:58 CST

Of course, this problem is as old as bank vaults, where the security interest requires that only one person know the combination but other interests require that in the event of his death the vault can still be opened by non-destructive means.

I think that a review of the market will demonstrate that "modern security and cryptography" meet this requirement where it exists. The reader who thinks otherwise should compare PGP, intended for personal use, to PGP Business Edition.

The former does not include any emergency key recovery while the latter does. Because of my profession, my age, and my failing memory, I choose to use the latter and its features. For the same reason, I choose to use RSA Secure which not only makes my file encryption automatic but also provides emergency key-recovery features.

It should be pointed out that these features (unlike proposals by the Clinton administration) provide me with arbitrarily strong protection against abuse by the trustees. They permit me to name an arbitrary number of trustees and require an arbitrary number of them to cooperate to recover the key that I have used. The higher the number that I name,

the lower the probability that they will be unavailable when needed. The more of them that I require to participate in the recovery, the lower the probability that the requisite number will behave inappropriately.

Two examples may help. For the protection of my file system, I have named two trustees. Since I carry my file system with me, sleep with it under my pillow, and am more concerned about the behavior of my memory than the ethics of my colleagues, either of them acting unilaterally can recover my key.

It should also be pointed out that I do not use these techniques for those keys that I use only for communication security. They are restricted to those that I use for file encryption. If I should forget the passphrase used to protect my communication private key, the appropriate remedy is to revoke the old public key, generate a new key pair and publish the new public key. If there are messages that I received but cannot read, they must be resent.

Note that using emergency key recovery for communication keys is not secure and may compromise my correspondents. It is at best rude and may violate my obligations to them.

Consider by contrast the master key for a major credit card company. This key was generated under rigorous conditions inside a hardware box called the BBN Safekeyper. It is a property of this box that it resists all

attempts to remove the private key from the box. Beneficial use of the private key requires possession of the box and all three of the physical keys that fit the three locks on the box.

Since the box is subject to physical destruction and since loss of use of the key would be disruptive, not to say destructive, the box published five numbers such that another Safekeyper box could reconstruct the private key from any three of the numbers. Thus, any three of the trustees could prevent the recovery. Of course, the values five and three are arbitrary but they are also illustrative. If 3 out of 5 works for this very sensitive application, it is difficult to imagine an application for which a larger number of trustees are required.

A security professional cannot recommend that important keys be stored in any other way. While I may consent to other arrangements, I recommend that important (usually master) keys be stored in hardware dedicated to that purpose with 3 out of 5 emergency key reconstruction.

Modern key management enables us to meet all of the security requirements and without creating new problems of their own. Any suggestion to the contrary is, at best misleading.

There appears to be an active campaign on the part of the government to pretend that these techniques do not exist and need to be invented. There is also a pretense on their part that the same remedies are necessary and appropriate for communications applications as for file

applications. As I
have attempted to show, the remedies for one are inappropriate
and insecure
for the other. Because the government insists upon pretending
to an untruth
where they must be presumed to know the truth, we should
seriously question
their motives.

William Hugh Murray, CISSP New Canaan, Connecticut

Protean documents

"Daniel P. B. Smith" <dpbsmith@world.std.com>
Sat, 21 Dec 1996 10:08:18 -0500 (EST)

Roland Giersig's remarks reminded ([RISKS-18.70](#)) me of a whole
spectrum of
issues that arise when one user creates a document and another
user *on
another computer* tries to edit it. Frequently, a significant
portion of
the document's state or structure are contained in various
preference,
configuration, and initialization files, or in the state of the
system
itself (what fonts are installed, what printer is selected,
etc), and
surprising transformations occur when the document is
transplanted into a
different user's computer.

The war story: the urgent proposal had to go out immediately; X,
who
prepared it, was out; Y was frantic because when she opened the
fifty-page
proposal on her system, everything that should be in boldface
was plain, and
everything that should be plain was bold.

What had happened was that, in some mysterious manner, X's NORMAL.DOT default style sheet had somehow gotten into a state where the normal style had the bold attribute. X had vaguely wondered for months why her word processor "always comes up in bold," but she just typed CTRL-B and went merrily onward. The "bold" attribute applied to text is exclusive-ored with the bold attribute from the style sheet, so everything seemed normal; when she thought she was applying bold, she was really removing it from the text (and allowing the style sheet "bold" to take effect), and vice versa. So all documents created by X had bold and plain swapped when viewed or printed on anyone else's computer.

Daniel P. B. Smith dpbsmith@world.std.com

[Protean = readily assuming different shapes or roles.
(Webster's) PGN]

✉ Re: Problems of "unforeseen" system aging (Brown, [RISKS-18.70](#))

<Andrew Koenig <ark@research.att.com>

Mon, 23 Dec 1996 10:12:08 +0500

Once upon a time I read an article by one Gerry Weinberg, who might have been the same Gerry Weinberg who wrote the excellent book 'The Psychology of Computer Programming.' In the article, he said that he was running a company that wrote applications software for other companies,

and that his standard practice was for all programs he delivered to have a stipulated lifetime of five years unless there was an explicit agreement otherwise.

The client agreed that at the end of the program's lifetime, either the client would pay to have the program refurbished or all copies would be destroyed.

Andrew Koenig ark@research.att.com

✉ Re: Problems of "unforeseen" system aging (Brown, [RISKS-18.70](#))

"Paul E. Bennett" <peb@transcontech.co.uk>
Mon, 23 Dec 1996 11:03:33 GMT

As one of many engineers in the Safety Critical Systems Arena I have seen such specifications. The normal lifetime expectancy for equipment (in harsh environments) is thirty years. After this time the equipment may need to be refurbished and continue another twenty years.

Such extended lifetimes do cause some problems, especially in trying to source components that can last that long (large capacitors are especially difficult). For this reason (among many others) many systems for such extended life embedded applications are becoming networked solutions. By networking, replacement sub-units can be installed that take advantage of the newer components available but able to work together with older

technology units.

This approach, of course, raises a whole set of new risk elements.

Paul E. Bennett <peb@transcontech.co.uk> Transport Control
Technology Ltd.
+44 (0)117-9499861

✶ Re: PCs and configuration management (Epstein, [RISKS-18.70](#))

Henry G. Baker <hbaker@netcom.com>
Sat, 21 Dec 1996 13:01:42 -0800 (PST)

Actually, the computer industry has (up til now) been surprisingly good at keeping model information/configurations consistent. The auto industry, on the other hand, has a dreadful record along these lines. Any car buff knows that auto manufacturers put whatever they had on hand into their cars, and the model number itself is merely one of many clues with which to start your search for the proper replacement part. Depending upon whose stuff arrived that morning, who was on strike that day, the phase of the moon, etc., you may get one of 3-5 different vendor's parts. I've even seen different vendor's parts on different sides of the same car! What's worse: the bracket may be different for each vendor's part, so that nominally interchangeable parts require sheet-metal work because the bolt patterns are different.

The worst example I've seen so far in ensuring consistency is Toshiba

laptops, where each model number has a different BIOS, and you aren't allowed to upgrade the disk to a larger disk_ (even if it is a Toshiba disk), because the BIOS won't recognize that size disk. The only way I could get the larger disk to work was to use Norton DiskEdit to set up the volume info to include one volume that the Toshiba BIOS liked, and made sure that that volume was the boot volume. The Toshiba employees who thought up this scheme should be rounded up and shot by the Dilbert patrol.

Henry Baker [ftp.netcom.com:/pub/hb/hbaker/home.html](ftp://netcom.com:/pub/hb/hbaker/home.html)

Microsoft documents and Rosetta stones (Giersig, [RISKS-18.70](#))

"Darrin B. Jewell" <jewell@mit.edu>
Sat, 21 Dec 1996 06:29:39 -0500 (EST)

This past summer I was getting increasingly frustrated by users who were sending me e-mail with Microsoft Word ".DOC" files attached to them via MIME encodings. I do not own a copy of Microsoft Word and did not want to purchase one simply so that I could read documents people send to me. Instead, I wanted the specification for Microsoft Word file format so that I would have a Rosetta stone for the documents I wished to read.

I contacted Microsoft's customer support and was informed of the following:

1. The specification for Microsoft Word file format is unpublished

proprietary information. However, I could download a free reader

for Microsoft Word files which would run under one of Microsoft's

operating systems. Source code for the reader was not available.

2. I could ask the sender of the message to send me the attachment encoded

in Rich Text Format which is the official export format for Microsoft

Word documents. The specification for Rich Text Format was publically

available from Microsoft.

Since I did not own a computer running one of Microsoft's operating systems,

I asked Microsoft for the specification for Rich Text Format files. As a

computer programmer, this was also a more useful and interesting form of

Rosetta stone than a precompiled translating program.

I was then directed to the file GC0165.EXE on the Microsoft ftp site, which

I was able to download and unzip. (Itself another decoding adventure.)

Included was the file GC0165.DOC, a Microsoft Word format file containing

the specification I desired. The included README.TXT file contained the

following comment in plain ASCII:

The GC0165.DOC file included in this compressed file is the Rich Text

Format (RTF) Specification version 1.3. The document is in Word 6.0 for

Windows format. If you have neither Word 6.0 for Windows nor Word 2.0 for

Windows with the 6.0-to-2.0 converter, you will need to call Microsoft

Product Support Services at (206) 462-9673 to obtain a hard copy of the

document.

At this point, I decided it was fastest to have my friend who owned Microsoft Word print out the RTF specification for me.

Since this experience, I usually ask people who wish to send me Word documents to send them in RTF format. When I explain to people the RISKS involved in using documents without open standards, I get comments about being ridiculous and pedantic or perhaps a blink and a "So what?" Even though Microsoft Word supports an "official export format", it is clearly not obvious to everyone why it should be used.

Darrin

⚡ Re: Arrogance of Micro\$loth Products (Giersig, [RISKS-18.70](#))

Bob Vaughan <techie@kzsu.Stanford.EDU>
Fri, 20 Dec 1996 18:02:44 -0800 (PST)

My personal experiences have shown that Micro\$loth software has some very severe compatibility problems.. - they are not even compatible with themselves.

Case in point: I recently designed lighting for a dance show, as part of the process, I needed to create a cue sheet for the stage manager to work from during the rehearsal process. Despite my extreme dislike for Micro\$loth in general, I decided that MS Excel for the Mac was the appropriate program to use. I proceeded to input my data for the first act, and saved

a copy on the desktop. I continued to input data, and saved a new copy (as a different name) on the desktop, as well as a copy to the CAP server on the nearby Sun workstation. I also printed 2 copies before closing the file. At this point, I had 2 printed copies, and (I thought) 2 online copies, on 2 different servers. I then grabbed a floppy disk, and went to copy the file to it so that I could work on it at the theatre the next day. However, when I went to grab the copy on the desktop (which had been saved not once, but two times!), I found that it did not exist, however the copy from the first act was there (with it's data intact, for the first act only). I then tried the copy stored on the CAP server, only to find that Excel would not open it as a Excel file, no matter how hard I tried.

I think the risks are obvious.

Another time, I was taking a class at a local community college, as part of the class, we were required to use Word for Windows (unknown version - this was several years ago, and my memory is a bit fuzzy). On several occasions, a file would get saved on a floppy disk, only to find that the file could not be opened by Word for Windows on any machine in the cluster, including the one that it had been created on. (This is typical of my experiences with Micro\$loth products in general)

As it turned out, I had almost as much knowledge about DOS/Windows as the instructor, and I try very hard to avoid DOS/Windows like the plague. My

purpose for taking the class, was to brush up my knowledge of DOS, against the increasing possibility that I would be asked to provide some support for DOS/Windows users (in spite of my hatred of DOS/Windows). As it turned out, the class did not go into DOS at all, instead concentrating on Windows applications, and not at all on the internals of the system itself. The class seems oriented towards future secretaries, and not towards users who wish to learn about how a computer system works. This was in spite of the course description, which implied that the class would be a general purpose introduction to the IBM PC.

The Risks? our society is rapidly turning out "trained computer users", who have no idea how the machine works, or even how to restart Windows from a DOS prompt.

Bob Vaughan, P.O. Box 9792, Stanford, Ca 94309-9792 techie@w6yx.stanford.edu
kc6sxc@w6yx.ampr.org techie@tantivy.net KC6SXC@W6YX.#NOCAL.CA.
USA.NOAM

✶ Re: Arrogance of Micro\$loth Products (Giersig, [RISKS-18.70](#))

"Jonathan I. Kamens" <jik@cam.ov.com>
Sat, 21 Dec 1996 20:25:05 -0500

With all due respect, I don't see how bugs in Microsoft products have anything to do with Microsoft's "arrogance."

I realize that a large segment of the computer-science community

likes to bash Microsoft at every opportunity. A good deal of that bashing may even be deserved. But it is hardly productive or responsible to take every single bug in a Microsoft product as proof that Microsoft is Evil. All that accomplishes is to evoke the "boy who cried wolf syndrome," thus causing real, legitimate complaints about Microsoft to be taken less seriously.

The last sentence of your message was rather indicative, I think. "Sorry if this sounds very emotional, but I have already wasted enough precious time with things like these." Yes, your message did "sound very emotional" -- in my opinion, inappropriately so. I'd like to think that the RISKS Digest is above petty anti-Microsoft grand-standing.

Jonathan Kamens OpenVision Technologies, Inc. jik@cam.ov.com

[So would I. PGN]

Secure passwords on the web? Not at Microsoft!

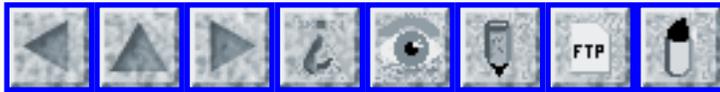
"Andrew Marc Greene" <amgreene@mit.edu>

Mon, 23 Dec 1996 11:23:11 -0500

I maintain a web site for the Zamir Chorale of Boston, and so I signed up at the Microsoft Site Builder network web site. Like so many others, it requires a username and password, and I used my standard "insecure" password -- that is, the one that I use at most similar sites. I certainly can't be bothered to remember which password goes with each of fifty web

sites that I
visit infrequently!

Well, I got USPS mail from the Microsoft Site Builder network
the other day,
encouraging me to visit their web site again -- and, just in
case I'd
forgotten my username and password, [Remainder of item
unnecessary for
regular RISKS readers.]



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 18: Issue 72

Monday 30 December 1996

Contents

- [Ontario legal system going online](#)
[J. Kivi Shapiro](#)
- [Do Not Attempt to use Airplane as Submarine?](#)
[Mark Brader](#)
- [Re: Cleaning person inadvertently kills patients](#)
[Mark Brader](#)
- [The risk of being clueless? ClariNet Site Audit](#)
[Mike Stump](#)
- [Beware - a new mail virus: PENPAL GREETINGS](#)
[Moshe Zviran](#)
- [Computer billing brouhaha for data networks](#)
[Robert Perillo](#)
- [Re: Microsoft documents and Rosetta stones](#)
[Henry G. Baker](#)
[Peter Bishop](#)
- [Re: Arrogance of Micro\\$loth Products](#)
[Robin Sheppard](#)
- [More Area Code Problems](#)
[Simson L. Garfinkel](#)
- [Re: Ghost 911 calls: software upgrade brings police](#)

[Michael Fuller](#)

[Peter Campbell Smith](#)

[Wayne Hayes](#)

[Steve Branam](#)

● [Re: Cookies](#)

[Marc Salverson](#)

● [Info on RISKS \(comp.risks\)](#)

✈ Ontario legal system going online

"J. Kivi Shapiro" <kshapiro@julian.uwo.ca>

Sun, 29 Dec 1996 18:44:36 -0500 (EST)

As a cost-saving measure, the justice system of the province of Ontario, Canada, has created a two-phase plan to file legal documents online rather than on paper as at present. The first phase covers civil courts; the second, criminal courts, police and correctional services. Documents to be submitted electronically in the first phase include various notices and statements of claim and defense, as well as court decisions.

The usual RISKS of relying on an electronic medium for important documents apply, with a twist. The proposed plan limits the accessibility of the documents: under the current system, they are generally accessible, but under the proposed plan, the lawyers involved with the case will decide whether or not to release them. This includes the statements of claim, explaining why someone is suing, and defense, the response from the person being sued.

The Canadian Press item I am using as a source quotes prominent Toronto lawyer Julian Falconer as saying, "a hallmark of a democratic process is the openness of the adjudicative process.... It is wrong and unseemly to put litigants and their counsel in the position of being gatekeepers of information." I am inclined to agree.

Kivi Shapiro

✈ Do Not Attempt to use Airplane as Submarine?

Mark Brader <msb@sq.com>
Sun, 29 Dec 96 01:08:09 EST

I was just reading a Transportation Safety Board of Canada report on a runway overrun incident in 1995 at Vancouver International Airport. The airport is on an island just barely above sea level; presumably, then, when a high pressure cell is in the area, its "pressure altitude" is below sea level.

>From the report (<http://bst-tsb.gc.ca/air/ea95h0015.html>):

1.16.7 Take-off Performance Below Sea Level Calculations

During the review of the take-off performance calculations for the flight, it was noted that the TPS incorrectly calculated the effect of below-sea-level pressures on engine performance. The manufacturer confirmed that the engine thrust curves indicated less thrust output

for operations at below-sea-level pressure altitudes; whereas the TPS program calculated that performance increased as pressure altitude decreased below sea level.

The CAI DC-10 FCOM and the OD43J Performance Manual also do not incorporate a performance-reduction correction for operations at below-sea-level pressure altitudes.

(TPS is the Takeoff Performance System computer, and FCOM is Flight Crew Operating Manual. CAI is Canadian Airlines International.)

Mark Brader SoftQuad Inc. Toronto

✶ Re: Cleaning person inadvertently kills patients ([RISKS-18.28, 18.29](#))

Mark Brader <msb@sq.com>
Fri, 27 Dec 96 16:26:22 EST

This past summer in [Risks-18.28](#), Michael Crawford reforwarded us an item beginning as follows:

| "For several months, our nurses have been baffled to find a
| dead patient in
| the same bed every Friday morning" a spokeswoman for the
| Pelonomi Hospital
| (Free State, South Africa) told reporters.

Michael didn't know if it was true, but he thought it sounded plausible. In the following issue, Prabhakar Ragde and Geoff Kuenning suggested that it sounded more like an urban legend, though a citation was given

for its
appearance in the Cape Times, a respected South African paper.

The following Web page:

<<http://www.legends.org.za/arthur/cleanfaq.htm>>

debunks the story thoroughly. It is indeed merely an urban legend.

Basically, it was circulating as a local rumor, and someone decided that it had better be investigated, since rumors are, after all, *sometimes* based on truth. The fact of the investigation then led to the story reaching the press and the Internet, and along the way the fact that it was *only* an investigation was lost.

Arthur Goldstuck, author of the Web page, provides not only successive versions of the story in Afrikaans and English, but also discussion with the newspaper staff involved. Recommended reading if you like that sort of thing.

Mark Brader SoftQuad Inc., Toronto msb@sq.com ["Oh, especially if it's accurate. There's nothing worse than *accurate*, ill-informed, irresponsible press speculation." -- Lynn & Jay: "Yes, Prime Minister"]

⚡ The risk of being clueless: ClariNet Site Audit

Mike Stump <mrs@cygnus.com>
27 Dec 1996 09:53:16 -0800

A friend forwarded this... It was sent to his system's `news' account... I think there are many risks. One is that you have a support staff that doesn't know why it would be bad, and sends him your site's root password via e-mail. Another is that this makes for a great spam scam for dishonest hackers... Another is that even if they are legitimate, it is a risk having passwords to many machines on the Internet in one location (prime target for dishonest hackers). I am sure I missed many risks as well. Oh, yeah, the risk on Clarinet having such an idea, and having them think it is a good idea.

----- Start of forwarded message -----

Date: Tue, 24 Dec 1996 14:50:44 -0800 (PST)

>From: Alex Ramos <alex@clari.net>

Subject: ClariNet Site Audit - Response Requested - Please Read

Dear Administrator:

You are listed in my records as ClariNet's technical contact at your site.

Our supplier contracts, the need for copyright protection and other

obligations require us to audit all sites and obtain confirmation of feed

data for our records on a periodic basis.

We have developed a two-step plan for implementing this audit, and we need your help to make this plan work.

As a first step, I have sent you a questionnaire to complete and e-mail back

to me. This should not take more than a couple of minutes, as it is simply

a listing of your newserver information and data about sites to which you

feed the e.News.

The second part will involve remotely checking your news-server from our site, thus we will need a login account and password.

Login account name:

Password:

[...]

⚡ Beware - a new mail virus: PENPAL GREETINGS

Moshe Zviran <zviran@post.tau.ac.il>

Tue, 24 Dec 1996 15:41:13 +0200 (IST)

>Forwarded virus warning!!!!!!!!!!!!

>

>If anyone receives mail entitled: PENPAL GREETINGS! please delete it

>WITHOUT reading it. Below is a little explanation of the message, and

>what it would do to your PC if you were to read the message.

>

>This is a warning for all internet users - there is a dangerous virus

>propagating across the internet through an e-mail message entitled "PENPAL

>GREETINGS!". DO NOT DOWNLOAD ANY MESSAGE ENTITLED "PENPAL GREETINGS!"

>

>This message appears to be a friendly letter asking you if you are

>interested in a penpal, but by the time you read this letter, it is too

>late. The "trojan horse" virus will have already infected the boot sector

>of your hard drive, destroying all of the data present. It is a self-replicating virus, and once the message is read, it will AUTOMATICALLY

>forward itself to anyone who's e-mail address is present in
YOUR mailbox!
>
>This virus will DESTROY your hard drive, and holds the
potential to
>DESTROY the hard drive of anyone whose mail is in your in box,
and who's
>mail is in their in box, and so on. If this virus remains
unchecked, it
>has the potential to do a great deal of DAMAGE to computer
networks
>worldwide!!!!
>
>Please, delete the message entitled "PENPAL GREETINGS!" as soon
as you see it!
>And pass this message along to all of your friends and
relatives, and the
>other readers of the newsgroups and mailing lists which you are
on, so
>that they are not hurt by this dangerous virus!!!!

Moshe Zviran, Faculty of Management, The Leon Racadati School of
Business
Administration, Tel Aviv University, Tel Aviv 69978 ISRAEL +972-
3-6409671

🔥 Computer billing brouhaha for data networks

<Perillo@DOCKMASTER.NCSC.MIL>
Mon, 30 Dec 96 10:29 EST

Many organizations have switched from Private Data Networks to
Carrier based
data communications services, such as the AT&T frame-relay
service. To take
advantage of the benefits of not buying, managing, and
maintaining their own
systems. Yet the automated billings for these services have had
many

errors. In a July user group meeting, user's talked of three years of bills with constant errors, and of monthly bills being off by as much as \$1,000 to \$2,000.

Originally, AT&T stated that the bills were correct, and the problem was that users were being fed inaccurate network loading and performance data. Users were using this incorrect data to track and double check the bills. In July, AT&T Corp. confirmed that flawed software in the StrataCom IPX network switches have provided users with inaccurate performance data. The software in the StrataCom (now acquired by Cisco) switches, that supports the Customer Network Management Services (CNMS), was said to have bugs and flawed algorithms.

AT&T sent a letter during the summer to all user's alerting them of the problem and warned them not to calculate usage, performance, or capacity using this corrupted data. AT&T stated that they became aware of the problems with the switch software in early 1996, and that they would be fixing the problem with either corrective software or by upgrading to StrataCom BPX switches by the end of 1996.

AT&T then admitted that their own billing process, an automated billing system in its new frame-relay network, was creating "billing blunders". AT&T blamed human error, and system integration problems. It seems that salesman were unable to enter contracted discounts into the automated system, and that facilities unrelated to the company's frame-relay service

were being included by the automated billing system essentially double billing.

Some user's stated that "the scary part is that these software anomalies somehow slipped through testing by StrataCom and AT&T, that shows that their system is not foolproof, and that is more of a concern than the corrupted data". Also, "If bills are incorrect, the service is perceived by users as being less trustworthy".

I have noticed that Performance Monitoring (PM) software is usually left to late in the development process, staffed by the less experienced or less productive engineers of the development team. Yet PM software can be tricky to develop, because you are trying to devise algorithms to measure a system that is still undergoing development and not completely defined. Also, it is very difficult to specify performance, how you measure it, and to not degrade performance by measuring it. It is difficult to test, because of the varying conditions and loads.

It is reasonable that the designers, concerned about the mission critical portions of the system, would concentrate their scarce resources in those area's. When I have brought these concerns up in team meetings, I have been told by project managers that we must focus on getting the system working first and that we can worry about meeting PM requirements "sometime down the road".

This attitude seems to create the Risks mentioned above, PM

software should not be the stepchild of the development effort. Because the first version of the PM software is usually incomplete and has bugs, it does not show complete system performance correctly. There have been projects that I have been on which have been out in the field for years, when we finally get the PM software working, we notice that the system has never been performing properly. Properly functioning PM systems can uncover flaws in the mission critical portions of the software and system.

REFERENCES

ComputerWorld, "Bug causes AT&T switch itch", 8-Jul-96, page 6.

ComputerWorld, "Billing brouhaha bristles AT&T frame-relay users", 15-Jul-96, page 8.

Robert Perillo, CCP Richmond, Va Perillo@dockmaster.ncsc.mil

✉ Re: Microsoft documents and Rosetta stones (Jewell, [RISKS-18.71](#))

Henry G. Baker <hbaker@netcom.com>
Mon, 23 Dec 1996 16:38:55 -0800 (PST)

Re: Internet Docs and the RTF spec/M\$Word recursion:

I ran into exactly the same recursion, but I took the more drastic/expensive route of purchasing Mac M\$Word 6.0.1c. Although this helped somewhat, it didn't completely solve the problem.

* Although the Mac/PC versions of M\$Word are roughly the same (I think that the bulk of this product is some kind of interpreted P-code) there are important differences -- e.g., they don't have the same capabilities to translate documents & graphics. Thus, if someone posts/e-mails a M\$Word document, you may be able to read the text, but the graphics may remain untranslated/invisible. Also, the PC versions of the fonts in the documents prevail, so printing on your Mac takes forever because the generated postscript includes separate commands _for each individual character output_! Oh, and BTW, the Mac version is unusable as a word processing program due to its incredible slowness, so it is _only_ good for translating documents and printing them.

* You should search a bit further. There are sites with the latest RTF spec in RTF format. They also have the earlier versions of the RTF spec, so you can see how it has changed.

* Having RTF won't necessarily help you. Although RTF is supposedly an 'open' format, many of the features are supported only by M\$Word, so you'll _still_ need access to M\$Word to read the document. Although there is supposed to be some level of backward compatibility, M\$Word doesn't work very hard at this, so the documents may still come out looking like a disaster.

* The posting of documents in a proprietary/trade secret format _by

government agencies at all levels_ should be illegal. Although M\$ provides a free Word reader for the PC, they provide no such reader for the Mac (or Un*x). The posting of court decisions in the proprietary wordperfect format is also a major irritant. If people can't easily read the document, then the agency has not made the document accessible.

* There are a number of 'conversion' programs available that supposedly handle RTF, Word X.X, Wordperfect, etc., documents. Some of them do a better job on the graphics than do the M\$ converters. However, most seem to do very poorly on the word-processing parts -- e.g., fonts, section headings, indentations, etc. So you may have to utilize an ascii editor to disassemble the RTF into text and graphics, convert each separately, and then put the mess together again. This is possible for one or two documents, but not something you want to do on a routine basis.

So far, html 1.0 & .gif appear to be more easily transportable than any particular word processing format, TeX excepted. Sadly, html is no closer to having a math capability than 3 years ago -- putting equations in gif's is not resolution independent!

Postscript is quite transportable, but many PC (l)users don't have Ghostscript or equivalent to print it on their HP-compatible printers.

PDF (Adobe) is quite transportable and there are good versions for the PC and the Mac. I commend the IRS for making their forms so readily available

on the Internet in this format.

Henry Baker www/ftp directory: ftp.netcom.com:/pub/hb/hbaker/home.html

⚡ Re: Microsoft documents and Rosetta stones (Giersig, [RISKS-18.70](#))

Peter Bishop <pgb@adelard.co.uk>

Tue, 24 Dec 1996 15:32:57 +0000

This is not a particularly deep comment, but one way of getting portable documents from Microsoft products is to install a Postscript driver under Windows. Choose this as the default printer and select the "print to file" option when printing.

I have used technique to to publish Postscript documents on our Web site.

Anyone with a Postscript viewer (such as the excellent Ghostscript) or a Postscript printer is then able to view the document regardless of the computer or operating system they use.

Peter Bishop, Adelard, 3 Coborn Rd, London E3 2DA, England
+44-181-983-0219 pgb@adelard.co.uk <http://www.adelard.co.uk>

⚡ Re: Arrogance of Micro\$loth Products ([RISKS-18.70](#))

Robin Sheppard <robshepp@napanet.net>

Tue, 24 Dec 1996 11:45:49 -0700

Without defending Microsoft, I would have thought that "the final lesson learned" should have been to read the manual.

It's easy to blame a software publisher when things go wrong with a program because of a programming error. Unfortunately, it's just as easy to blame the publisher when things go wrong through user ignorance. An increasing number of "risks" reported here seem to fall into the category of "I was driving my car at 120 mph when I hit a patch of ice and slammed into a tree, and it's all Ford's fault."

By all means, criticize the publisher when there is an error in a program; but accept personal responsibility for user errors.

Robin Sheppard

✈ More Area Code Problems (Re: Kay, [RISKS-18.71](#))

"Simson L. Garfinkel" <simsong@vineyard.net>
Tue, 24 Dec 1996 13:38:42 -0800

I read Timothy L. Kay's problem with his paging software calling the police. One of the real problems, I think, is that we don't really have a national consensus about phone numbers, area codes, and country codes:

- * Is my phone number 555-1212, 617-555-1212, or 1-617-555-1212?
- * Should the phone system allow me to dial 1-617-555-1212 if I am in area code 617?

I'm having this problem in spades right now in a cross-country trip that I'm taking. Some cell phone areas that I drive through require that you dial 1-617-555-1212. Others insist that you dial 617-555-1212. You can imagine that this means that my stored phone numbers don't work half the time, depending on which zone I'm in.

Frankly, I think that the ambiguity over area codes and the "1" is an industry disgrace and its sure to cause billions of dollars in lost productivity and lost time over the coming years. But I don't see any way to resolve the problems. When I speak with phone companies about this matter---I ask them "why don't you let people always dial 1+area code even when you are in the area code"---they don't even have a clue what I'm talking about.

I have an OP-ED piece that I wrote on a similar subject --- area code splits -- and I will post it if there is interest.

-simson

Follow Simson's ramblings at <http://www.packet.com/garfinkel>

⚡ Re: Ghost 911 calls: software upgrade brings police (Kay, [RISKS-18.71](#))

Michael Fuller <msf@dgs.monash.edu.au>
Tue, 24 Dec 1996 12:24:42 +1100

Timothy has fallen into the trap of being US-centric. "911" is

the
emergency services telephone number in the US. But in
Australia, "911"
doesn't mean a thing - our equivalent is "000". "911" would
simply be the
first three digits of a normal local telephone number! [AUSTEL
policy may
preclude this, but not as far as I can see. For reference, see
<http://www.austel.gov.au/info/numbering/>]

Other countries use other things - a quick search of the New
Zealand Telecom
WWW site revealed that they use "111". I'm sure that there
numerous other
variants. Now, unless modem manufacturers want to supply an
appropriately
tailored setup for every country in the world (and they'd better
make sure
they get it right!), then it's ridiculous for them to consider
about
building in such checks.

Note that if "911" *was* the appropriate emergency services
contact number,
to block modem calls to it would eliminate potential systems
that might be
designed to watch over the elderly or infirm, and automatically
contact
emergency services when appropriate, security systems that might
do the
same, and so on.

So, no, it would not make sense to include a "911" sanity check;
to do so is
arguably a RISK in its own right.

Michael Fuller

[I was thinking more of a context-sensitive parameter-
programmable
advisory rather than a complete blockage. I should have been
much more
explicit. However, the theme of Timothy Kay's US-centricism

was noted by

quite a few others, including

Sebastian Delmont <sdelmont@planetaurbe.com>

(in Venezuela, 91 is an area code).

Terje Mathisen <Terje.Mathisen@hda.hydro.com>

(in Norway, 911xxxxx is a mobile-phone number,

although 900MHz GSM phones will never work in the US

anyway!)

Tim Kuehn <timk@tdkcs.waterloo.on.ca>

(in Canada, one must dial 1 even within an area code!)

Also,

"Andrew Marc Greene" <amgreene@mit.edu> noted that in the 617 area-code

in Massachusetts, some intra-617 calls require a preceding 1. Etc.

The moral lesson is a familiar one in RISKS: Easy answers are risky.

Complex solutions are also risky. On the other hand, even moderate

solutions are risky, as your immoderate moderator repeatedly points out.

So, join the RISKS club. By the way, any automatic censorship technique

is likely to run afoul of similar difficulties! PGN]

[Re: Ghost 911 calls: software upgrade brings police \(Kay, RISKS-18.71\)](#)

"Campbell Smith Peter (Exchange)" <CAMPBELLP@logica.com>

Tue, 24 Dec 1996 13:45:42 -0000

[... 112 spreading for emergencies ... 911 is prefix for a London university]

* Phone numbers change so quickly these days that any assumptions built into software are likely to be invalid in a few years.

* Some address book applications use modems to dial telephone

numbers for
voice calls. No doubt there's one out there with an 'emergency'
button, and
I wouldn't be too happy to discover that the modem had
suppressed the number
as my house burnt down around me.

Peter Campbell Smith, Logica, London, UK
campbellp@logica.com - phone:+44 171 446 4496 - fax:+44 1932
869107

✉ Re: Ghost 911 calls: software upgrade brings police (Kay, [RISKS-18.71](#))

Wayne Hayes <wayne@cdf.toronto.edu>
Tue, 24 Dec 1996 11:21:05 -0500

I'm sitting in front of my computer and have a heart attack. I
can't get to
the phone in the other room, so with my last ounce of strength I
fire up my
modem software and type "atdt911". When my house-mate arrives
later that
day to discover my dead body and

atdt911

ERROR

on my screen, a law suit against the modem manufacturer would
almost
certainly ensue. One could even envision some sort of automatic
system that
might require a modem to dial 911.

If there's one thing your post shows, it's that adding needless
complexity
to a software system (a.k.a. making the software "smarter")
often adds

confusion and can lead to Really Bad Things.

⚡ Re: Ghost 911 calls: software upgrade brings police

Steve Branam <branam@dechub.lkg.dec.com>

Mon, 30 Dec 1996 13:34:01 -0500

Two years ago I had a similar incident. I had received a set of operating system upgrade disks for a home system, primarily intended to correct some problems in some of the items bundled with it. The upgrade went smoothly and shortly after I attempted to dial up my online service provider. I heard the modem dialing, but rather than the full dialing sequence, a person quickly came on the line and said, "Emergency 911." Yikes! The modem continued sending digits for a second while I sat there totally confused. The emergency operator did not wait very long before hanging up.

I then waited for a return call or the police to show up. Neither occurred. Meanwhile, I checked my comm setup. Where before I had disabled "9" for outside line access, it was now enabled. In addition, the prefix "1174" (or some similar meaningless code beginning with "11") was specified to disable call waiting. Thus the setup specified the full prefix "91174" before the actual number; the switching system cut me over to the 911 operator as soon as the second 1 was sent.

Prior to the upgrade, I had been able to dial in with no problems. Since I had not changed the setup, I concluded that the upgrade had;

226-6043

✉ Re: Cookies (Stuart, [RISKS-18.68](#))

Marc Salverson <marc@colsa.com>

Tue, 24 Dec 1996 10:53:48 -0600

Is the setting "2" or "not 1 or 0"? What about the RISK of Netscape adding option 2 = "don't accept cookies from strangers & send password file", or any other option you might not want to choose by default but already have chosen by setting the option to "2"?

Marc Salverson <marc@colsa.com>, Network Analyst, Advanced Research Center (ARC)



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 18: Issue 73

Monday 30 December 1996

Contents

- [HOAX: PENPAL GREETINGS](#)
[Michael Kohne](#)
- [China Strengthens Control Over Internet](#)
[Edupage](#)
- [Re: Action Alert](#)
[David Wittenberg](#)

✶ HOAX: PENPAL GREETINGS (Re: Zviran, [RISKS-18.72](#))

Michael Kohne <mhkohne@discordia.org>
Mon, 30 Dec 1996 15:28:18 -0500

SIGH. Don't we get enough of these in the newsgroups? This is yet another variation of the good-old Good Times hoax virus. Checkout <http://www.symantec.com/avcenter/vinfodb.html>. The 'P' section contains an entry on this annoyance.

As a general warning to everyone out there - Please do NOT pass

along
virus/trojan/etc warnings to ANYONE until you have discussed the
matter
with your sysadmin. Your sysadmin will likely know if it's real
or not, and
will be able to help you take proper preventive measures, and
distribute
the warning properly.

I know you are trying to help by distributing this warning, but
really, all
you are doing is WASTING EVERYONE'S TIME!

Thank you.

[Similar rapid responses on the hoax also contributed by
Michael Naunton <mmn@onyx.interactive.net> and
Al Stangenberger <forags@nature.berkeley.edu>, who pointed
to

<http://ciac.llnl.gov/ciac/CIACHoaxes.html>

Too bad we were not approaching 1 April instead of 1 Jan. PGN]

✶ China Strengthens Control Over Internet (Edupage, 29 Dec 1996)

Edupage Editors <educom@elanor.oit.unc.edu>

Sun, 29 Dec 1996 18:19:39 -0500 (EST)

The newspaper called *China Consumers Daily* says that China plans to increase its controls over the Internet, which already include the requirement that all Internet users register with the police. In its war against pornography and "cultural rubbish," Chinese police detained more than 47,000 people and seized 320,000 pornographic products in the first ten months of 1996. Chinese authorities use the term "cultural

rubbish" to include anything they consider unhealthy or politically suspect. (*Atlanta Journal-Constitution*, 27 Dec 1996, D3)

⚡ Re: Action Alert (Handler, [RISKS-18.71](#))

David Wittenberg <dkw@cs.brandeis.edu>
Mon, 30 Dec 1996 14:31:46 -0500 (EST)

In [RISKS-18.71](#), Jon Handler warns of the spread of personal information on the net, and gives the URLs of several suppliers of such information.

A longer list is available from "The Stalker's Home Page" <<http://pages.ripco.com:8080/~glr/stalk.html>> It's a rather scary resource for finding people or information about them.

--David Wittenberg dkw@cs.brandeis.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 18: Issue 74

Tuesday 7 January 1997

Contents

- [U.S. Air Force webpage hacked](#)
[PGN](#)
- [Grammy web page leaks nominees](#)
[B.J. Herbison](#)
- [The Sky Is Falling](#)
[Jim Horning](#)
- [Computer safety 25 years ago](#)
[Wayne Hayes](#)
- [Leap-Year software bug gives "Million-dollar glitch"](#)
[Jim Towler](#)
- [VISA fines banks with Y2K problems](#)
[Lloyd Wood](#)
- [Y2K: Blessing in Disguise](#)
[Mark Brader](#)
- [Another privacy bug in Netscape](#)
[Kevin McCurley](#)
- [When connectors shouldn't meet](#)
[Lauren Weinstein](#)
- [Dan Farmer releases real-time security survey](#)
[Betty G. O'Hearn](#)

- [Let UPS publish your signature on the Net Hall](#)
 - [Easy answers... Steve Hand](#)
 - [April 1 considered harmful William J. Evans](#)
 - [Re: Do Not Attempt to use Airplane as Submarine? Sam Lepore](#)
 - ['Ghost Trains' evidence of safe design Andrew Waugh](#)
 - [2nd FMICS Int. Workshop, Call for Papers Diego Latella](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ U.S. Air Force webpage hacked

"Peter G. Neumann" <neumann@csl.sri.com>
Mon, 30 Dec 1996 18:10 PDT

U.S. Air Force has now joined the club along with the Department of Justice, CIA, and NASA, whose webpages had previously been altered by intruders ([RISKS-18.35](#) and 49). On Sunday morning, 29 Dec 1996, the main webpage of the Air Force's website <http://www.af.mil> at Fort Belvoir, Virginia, was included ``Welcome to the Truth,' ' above dripping blood and a pair of red eyeballs, and ``You can learn all about gov't corruption here. Learn the secrets that they don't want you to know.' ' Also included were links to nonGovernment webpages and an X-rated picture with the caption, ``This is what your gov't is doing to you every day.' ' A person identified as a 23-year-old small-business man claiming to have been involved

with the two intruders said that they actually had access to the entire AF e-mail system (including classified documents), and were trying to show how 'pathetic' the security was. An AF spokesman suggested that they had access only to one PC. (Fort Belvoir also houses the websites for the Army and Marines.) [Source: Hackers Disrupt Air Force Web Page, article by Seth Schiesel, *The New York Times*, 30 Dec 1996.]

[Yes, the primary purpose of your webpage is usually to make information openly available, not to protect secrecy. But also don't forget that integrity and preventing denials of service are fundamental parts of your web and net security problems.

This case was also noted by Christopher Klaus <cklaus@iss.net>, who added 'With so many government web sites getting hacked, you think they would spend a little more time securing them. The tools exist to secure the web sites.' Well, more or less. PGN]

🔥 Grammy web page leaks nominees

"B.J. Herbison" <bherbison@HighGround.com>
Tue, 7 Jan 1997 10:42:06 -0500

On the CNN Interactive web site (cnn.com) today there is an article about the Grammy awards (www.grammy.com). The Grammy award nominees were supposed to be officially announced at 8:40 this morning, but the announcement was on

the web site overnight, removed early this morning.

When the Grammy site reposted the list, the names matched the information

from CNN. The CNN article is at

<http://cnn.com/SHOWBIZ/9701/07/grammy/index.html>

This is nothing new, just the standard risk of not integrating the standards

for new technologies with the existing technologies.

B.J. Herbison, HighGround Systems, Inc., 1300 Massachusetts Avenue

Boxborough, MA 01719-2203 bherbison@HighGround.com +1 508 263-5588 x126

⚡ The Sky Is Falling

Jim Horning <horning@intertrust.com>

Fri, 03 Jan 1997 10:46:00 P

The "Week in Review" in **The New York Times**, 29 Dec 1996, led off with a column by Michael Wines entitled "The Sky Is Falling: Three Cheers for Chicken Little." It will probably be of interest to most readers of RISKS.

I don't agree with all of it, but it is definitely thought-provoking.

I just excerpt the main points:

``'Time is running out,' ... Mr. Peterson is writing about the imminent bankruptcy of Medicare. No matter. It easily could have been global warming, overpopulation, designer genes, nuclear terrorism, AIDS, the national debt, Apple Computer, Democrats, Republicans, the two-party system,

wetlands, desertification, moral decline, moral zealots, killer asteroids
or, for that matter, software that does not recognize the year 2000...

``Alarmism is a national obsession... Are Americans getting too much of a bad thing? Of course they are. But that begs the real question: why doesn't the sky fall? And that question is a tougher one. Sure, plenty of alarms are raised over threats that are, to put it kindly, overstated... Maybe the sky doesn't fall because alarms work as the alarmists intended. Maybe the apocalypse never fully arrives because the alarmists' wretched excess frightens people into taking action...

``There's no way to know for sure. The only evidence that an alarm works is in its being proved false -- which may also be evidence that the alarm was unnecessary to begin with..."

``'It would be intellectually satisfying to say the real impact is through reasoned discourse,' [Paul Ehrlich] said. 'But in my view the real impact isn't in reasoned discourse. Media attention, press coverage and, if necessary, alarmism at least set an agenda. And that way you can have a debate.'" ...

``Alarmists can be self-promoting pains, and they are often wrong. So ignore them. How bad could life be on an Earth slow-cooking in a sauce of melted icebergs, populated by genetic experiments gone wild and fated to an eternity of Windows 95?"

Jim Horning

[Perhaps Cassandra was a little chicken rather than a Chicken Little? PGN]

🔥 Computer safety 25 years ago

Wayne Hayes <wayne@cs.toronto.edu>

Tue, 7 Jan 1997 14:50:36 -0500

I was rummaging around my old books recently and came upon the following gem. It is interesting to note that everything he says is still true today, down to the things he suggests we need to do to make software safer. And this was 26 years ago. When will we ever learn?

>From The Computer Revolution, by Nigel Hawkes. Copyright 1971 Thames and Hudson, London. Copied without permission.

HOW SAFE ARE COMPUTERS? (pages 193-196)

Less often discussed but potentially more serious is the danger of what I call computer-aided disasters. Many computer experts, particularly those in the software field, believe that these represent a very serious danger. Alex d'Agapeyeff, President of the British Computer Society, has argued that the existing computer systems have a reliability rather worse than that of the British telephone service. Other computer professionals have claimed that up to 70% of the computer systems in operation in Britain are unsuccessful. [He doesn't define what he means here.-WH] Although this may be an exaggeration, we would be wise to recognize the

widening gap between what the computer salesmen claim and what the systems engineers actually provide. Large computer systems remain something of an unknown quantity, and are quite capable of going very seriously wrong.

Most of the time this does not matter, except to those directly concerned. It is naturally irritating when a computerized system sends one an absurd bill, but it can usually be corrected without too much trouble. [And now, in 1996, even that is sometimes not possible.-WH] When computers are used to control jumbo jets, chemical plants or nuclear power stations, the effects of a similar failure might be catastrophic. More dangerous still, some people believe, are elaborate military systems, where relatively untried weapons may be sent on their way to the target by relatively untried software. The kind of dangers that can arise even in civil air-traffic control are epitomized by a story about Britain's new computerized system, called Mediator. As a first stage of implementation, a computer was introduced which could not deal easily with letters of the alphabet; instead it used flight numbers to identify aircraft. Soon after its introduction, three aircraft were circling over Watford waiting for clearance to land at Heathrow, and all three had the same flight number --- BEA flight 701, Air India flight 701 and Iberia flight 701. Fortunately, a human air-traffic controller noticed in time, before the computer had time to give all three aircraft clearance to land at once.

What security can one have against computerized disasters? Errors very rarely arise in the hardware of a modern computer.

Almost all are introduced by human error --- by carelessly written

programs, inaccurate input data or badly conceived systems design.

Greater emphasis on software development and improved input methods

would help, but alone are never likely to be enough. The dangers we

really need to worry about are exactly the ones we cannot predict,

and therefore cannot easily guard against. As a minimum, it seems

to me, we should insist on all major computer installations being

designed to 'fail softly' by falling back to a degraded state of

operation rather than collapsing catastrophically. In the case of

chemical plants, nuclear power stations, or medical intensive care

units, we should insist that the control function is so designed

that it can if necessary be taken over by a human operator in the

event of a computer breakdown. Failing that, a completely independent 'stand-by' system, with its own power supply, should be

installed. These may seem expensive safeguards, but they are cheap

compared with the possible costs of ignoring them.

Unfortunately, there are at the moment no agreed standard to which computer systems are expected to conform. The industry is

new, and growing fast, and nobody has yet taken the time to set up

proper disciplinary agencies. Even when these are established, they

are unlikely to be wholly effective, if the experience of other

industries is any guide. Most probably, a better safeguard

would be

to 'professionalize' the computer programmers by establishing learned institutions like those set up in the nineteenth century by

the engineers. The British Computer Society is, indeed, trying to

turn itself into such a body, although it still has a long way to go.

[And these topics have been discussed in the ACM Software Engineering

Notes now in volume 22, and RISKS for 11.5 years, ever since.

However, I do not recall this book being mentioned before. PGN]

⚡ Leap-Year software bug gives "Million-dollar glitch"

Jim Towler <jtowler@csi.co.nz>

Wed, 8 Jan 1997 09:47:40 +1300

Too many are suggesting that new programs are all OK and its only the "old mainframe stuff" that will have problems with "Year 2000". Well, people are still writing code with bugged date logic. Jim Towler, Wellington, New Zealand

Million-dollar glitch ("The Dominion" -- Wellington, New Zealand,

8 Jan 1997) via NZPA [New Zealand Press Assoc.]

A computer glitch at the Tiwai Pt [place in South Island of New Zealand]

aluminium smelter at midnight on New Year's Eve has left a repair bill of

more than \$1 million [New Zealand Dollars]. Production in all the smelting

potlines ground to a halt at the stroke of midnight when the

computers shut
down simultaneously and without warning. New Zealand Aluminium
Smelters'
general manager David Brewer said the failure was traced to a
faulty
computer software programme, which failed to account for 1996
being a leap
year. The computer was not programmed to handle the 366th day
of the year,
he said. "Each of the 660 process control computers hung up
simultaneously
at midnight," Mr Brewer said.

The same problem occurred two hours later at Comalco's Bell Bay
smelter, in
Tasmania [Australia]. New Zealand is two hours ahead of
Tasmania. Both
smelters use the same programme, which was written by Comalco
computer
staff.

Mr Brewer said the cause was difficult to trace and it was not
till a
telephone call in the morning from Bell Bay that the leap year
link was
made. "It was a complicated problem and it took quite some time
to find out
just what caused it."

Tiwai staff rallied through the night to operate the potlines
manually and
try to find the cause. The glitch was fixed and normal
production restored
by midafternoon. However, by then, the damage has been done.
Without the
computers to regulate temperatures inside the pot cells, five
cells
over-heated and were damaged beyond repair. Mr Brewer said they
would have
to be replaced at a cost of more than \$1 million.

[Reminder: I generally do *not* use a ``spellchecker'' for
Britishisms

(including Kiwi-isms) such as aluminium vs aluminum, honour, etc.

But here we clearly needed a ``smeltchecker'' for our Smeltschmertz. PGN]

⚡ VISA fines banks with Y2K problems

Lloyd Wood <L.Wood@surrey.ac.uk>

Tue, 7 Jan 1997 11:46:34 +0000 (GMT)

The article below appeared in The Times (London, UK), Mon Jan 6 1997,

Business News p41 first column, Article is probably available on The Times'

website at <URL:<http://www.the-times.co.uk/>> - registration is required, and

a quick hunt didn't turn it up.

BANKS FACE FINES OVER VISA CARD PROBLEMS, Fraser Nelson

Visa, the world's largest credit card company, is preparing to impose a fine

of up to UKP100,000 per month on some of its member banks in a last-ditch

attempt to ensure that they will accept credit cards with expiry dates

extending into the new millennium.

The company, itself a consortium of 20,000 banks, is launching the penal

system a year after its first deadline for Year 2000 compliance. It

estimated that 1.3 million outlets worldwide are still unable to deal with

cards with expiry dates reading '00'. Britain is believed to account for

only 40,000 of the faulty terminals.

After April, banks that have problems processing Visa's cards

will be charged between UKP600 and UKP100,000 per month, depending on volume, until they correct the bug.

Visa says that 90 per cent of terminals accept the new cards but an unacceptably high number still throw up an error when told a card was issued in '97 and expires in '00. Jim Dickie, vice president of Visa's operations and services in Europe, said the move was the next logical step to safeguard the credit card's brand name.

Year 2000 compliance is the first of three upheavals Visa faces over the next three years. The cards are also to have built-in microchips, and European monetary union will require further upgrades.

[My Visa card expires in March. I wonder if I'll encounter any of those 'only 40,000' terminals this year? Convincing shop assistants that my card isn't stolen could be an interesting experience. L.
<URL:<http://www.sat-net.com/L.Wood/>><L.Wood@ieee.org> +44-1483-300800x3435]

[And don't forget the scam this engendered, noted in [RISKS-18.68](#). PGN]

⚡ Y2K: Blessing in Disguise

Mark Brader <msb@sq.com>
Wed, 1 Jan 1997 18:55:50 GMT

I was in the Los Angeles area on October 20 and clipped this from the

Times [presumably LA, rather than NY, but I don't know Mark's habits.

PGN] that day, but forgot to send it along until now. Perhaps it's more appropriate on New Year's Day anyway:

| Your Oct. 16 editorial ("The IRS Wages War on the Millennium Bug")

| misses the point. The "Year 2000" problem is a blessing in disguise.

| Thanks to our computers we can relive the 20th century.

Think of

| the mistakes we can correct this time around. We can prevent two

| world wars, find Amelia Earhart, vote for Hubert Humphrey in 1968,

| catch the Unabomber before he strikes and tell young Jeffrey Maier

| to stay in his seat!

| Bill Smart, Santa Barbara, letter to the editor

[Disguise (DisGuy's?) the Limit.

And remember, tomorrow today will be yesterday -- at least until 31 Dec 99. PGN]

⚡ Another privacy bug in Netscape

Kevin McCurley <mccurley@swcp.com>

Sun, 5 Jan 1997 13:45:19 -0700

Version 2.0 of Netscape navigator had a bug in it that allowed web sites to

"steal" your e-mail address when you visited the page (see http://itu.rdg.ac.uk/misc/Mailing_Lists/cpd/0000002.htm). That

bug was

fixed in Version 2.02 by trying to require that the user approve any mail

that is sent out from their machine. Unfortunately, a new bug has been

discovered in Netscape 3.0, 3.01, and 4.0b1 that once again allows a web site to steal addresses from browsers without the consent of the user. A satirical demonstration of this is located at <http://www.digicrime.com/noprivacy.html>.

Such bugs continue to undermine the public's trust of the Internet. The existence of the bug is simply a programmer error rather than a malicious act. A far more insidious act is the exploitation of such mechanisms to steal e-mail addresses for unknown purposes. In fact the old 2.0 bug is still in use at a US government site:

<http://www.hr.doe.gov/ucsp/doeucsp.htm>

Kevin McCurley

⚡ When connectors shouldn't meet

Lauren Weinstein <lauren@vortex.com>

Fri, 3 Jan 1997 15:53 PST

The latest (Jan 1997) issue of "Mix" magazine (a pro-audio trade publication), points out a potential risk in some new connectors recently introduced for the audio industry. Essentially, these are a set of adapters that convert common audio connectors to the standard three prong A.C. power configuration. The idea is to allow ordinary power extension cords to be used to carry audio in "emergency" situations at wiring performance venues if the "correct" cable isn't available.

Mix properly notes serious concern over the obvious risks of such use, especially in the hectic wiring situations where mislabeled cables are common, and a technician thinking he or she was handling an audio cable might find themselves plugged into A.C. mains current instead.

Lauren, Moderator, PRIVACY Forum www.vortex.com

⚡ Dan Farmer releases real-time security survey

"Betty G. O'Hearn" <betty@infowar.com>

Mon, 06 Jan 1997 00:27:15 -0500

Dan Farmer, security researcher and creator of SATAN, just released the results of a real-time security survey on the Internet. It included various classes of attacks against government sites, 660 world wide banks, credit unions, on-line sex businesses and media orgs.

WWW.InfoWar.Com has posted the complete survey. There is no charge for complete access to this invaluable, unauthorized survey.

Click on the home page of www.infowar.com at the icon "New on Infowar.Com" - Scroll down. The survey is listed at 2 Jan 1997.

[SATANic curses? PGN]

⚡ Let UPS publish your signature on the Net

<hall@alvoid.research.att.com>

Mon, 6 Jan 1997 14:31:48 -0800 (PST)

I noticed a UPS (United Parcel Service) TV commercial this weekend that advertises the capability for one to download an image of the signature of the person who signed for a package. It seems like a matter of a few minutes of hacking for a reasonably clever forger to gain the ability to sign checks and credit card slips (particularly those you sign and mail in) on behalf of anyone who signs for a UPS package. Even if there is tight network security so that only the package sender can see the signature, nothing stops a would-be forger from UPS-ing a bogus package to the person whose credit card or checkbook s/he stole.

To the extent that handwritten signatures are used as a security measure any more (which is debatable, of course), publishing them in a computer-readable medium seems to me like an unnecessary risk with little or no compensating advantage.

-- Bob

[Ah, yes, we have been around on this one before.
See [RISKS-11.42](#), 11.71, and 15,29. PGN]

✶ Easy answers... (PGN, [RISKS-18.72](#))

Steve Hand <sassth@unx.sas.com>

Mon, 6 Jan 1997 14:16:03 -0500 (EST)

> The moral lesson is a familiar one in RISKS: Easy answers are

risky.

> Complex solutions are also risky. On the other hand, even moderate

> solutions are risky, as your immoderate moderator repeatedly points out.

And, as newspaper editor H.L. Mencken said, "For every complex question there is a simple answer, and it is wrong."

Steven Hand sassth@unx.sas.com
(919) 677-8000 ext. 6936 (work) 847-9354 (home)

✶ April 1 considered harmful

William J. Evans <wje@netcom.com>
Mon, 30 Dec 1996 13:29:58 -0800

Our esteemed PGN commented with respect to the alleged PENPAL virus:

: Too bad we were not approaching 1 April instead of 1 Jan.

We need to address the risks involved in even having a 1 April in the calendar. What if a powerful newbie takes a 1 April prank seriously, and dives in to "fix" something? What are the risks there?

Alternatively, what are the risks of expanding March to 32 days and starting April with 2 April?

Would that be any worse than the upcoming Y2K?

Sorry, but I couldn't wait three months to submit this. Too bad we're not approaching 1 April instead of 1 Jan.

Bill Evans/Box 4829/Irvine, California 92716/(714)551-2766
wje@acm.org

✶ Re: Do Not Attempt to use Airplane as Submarine? (Brader, [RISKS-18.72](#))

<Sam.Lepore@ncal.kaiperm.org>

Tue, 31 Dec 1996 12:08 PST

> The airport is on an island just barely above sea level;
> presumably, then,
> when a high-pressure cell is in the area, its "pressure
> altitude" is below
> sea level.

As amusing as it may seem, this shows the excellent design of
being prepared
for an unlikely event - like flying below sea level. Unlikely,
but not
impossible.

This reminds me of an unconfirmed report from many years ago
about the first
military aircraft from China Lake/Edwards AFB that flew with an
altimeter-linked autopilot and tried to buzz the deck in Death
Valley (280
feet below sea level). I've heard various stories about it 1)
tried to land
in mid-air; 2) believed it was about to crash and attempted to
eject the
pilot; 3) nearly flew into the Panamint mountains trying to
avoid crashing
at 'sea level'.

[Mark Brader received an out-of-band message from
Richard.Black@cl.cam.ac.uk
reminding him that one of the busiest airports in the world
(Amsterdam
Schipol) is (like much of the Netherlands) below sea level.
PGN]

✶ 'Ghost Trains' evidence of safe design (PGN, [RISKS-18.70](#))

<A.Waugh@mel.dit.csiro.au>

Thu, 2 Jan 1997 15:11:28 EST

Without further details, it is almost certain that the 'ghost train' is a track circuit failure.

Track circuits are the fundamental building block of railway signaling systems. Their purpose is to detect the presence of a train in a particular section of track. Failure to detect a train is certain to eventually cause a serious accident; the Clapham Junction accident in the UK, for example, was caused by a wiring error which omitted a track circuit from the controls of a signal.

All technology fails, of course, so track circuits are designed to indicate the presence of a train when they fail. This is 'safe' as it holds signals at danger and prevents any points in the track section from moving.

Totally locking up the system, however, would close the line until the track circuit was repaired. So there is always a method of granting authority for trains to pass a signal at danger and *slowly* pass over a track when a track circuit fails -- the 'manual operation' mentioned above. The railways have traded off a small amount of safety (a small number of collisions have occurred when Drivers travel too fast under these circumstances) to prevent

total closure of the line.

The 'ghost train' in the tale is the result of a deliberate decision as to a technology failure mode, careful design to bias potential failures into this safe failure mode, and a careful trade off between safety and closure of the line. Given the very low accident rate on railways equipped with track circuits, the 'ghost train' is, in fact evidence of a Risk success, not a failure!

andrew waugh

[We received a ton of e-mail on ghosts, 911, etc., lots of minor variants on earlier themes, far too many to include here. TNX. PGN]

✶ 2nd FMICS Int. Workshop, Call for Papers

Diego Latella <latella@sting.cnuce.cnr.it>
Tue, 7 Jan 1997 11:38:10 +0100

Second International Workshop on Formal Methods for Industrial Critical Systems
ERCIM - FMICS CESENA (Italy) 4-5 July 1997
[truncated for RISKS]

The Second International Workshop on Formal Methods for Industrial Critical Systems will take place in Cesena, close to Bologna (Italy) as a Satellite Workshop to the 24th International Colloquium on Automata, Languages, and Programming, ICALP '97. Workshop page URL:
<http://fdt.cnuce.cnr.it/~latella/FMICS/WS/Cesena97/workshop>.

[html](#)

The aim of these workshops is to provide a forum mainly for, but not limited to, researchers of ERCIM Sites, interested in the development and use of Formal Methods in the Industry. In particular, these workshops should bring together scientists active in the area of formal methods and willing to exchange their experience in the industrial usage of these methods. They also aim at promoting research and development for the improvement of formal methods and tools with respect to their usage in/interest of industry. Please notice that the workshop will be held in conjunction with the Second International Workshop on Advanced Intelligent Networks (AIN'97)

SUBMISSIONS: Authors are invited to send five copies of a full paper (in English, up to 25 pages) to the Programme Chair: S. Gnesi, CNR - Ist. Elaborazione dell'Informazione Via S. Maria 46, I56126 Pisa - ITALY by 31 JAN 1997. An electronic version of the paper in .ps format plus an abstract should also be sent to: fmics@iei.pi.cnr.it



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 18: Issue 75

Friday 10 January 1997

Contents

- [Newt Gingrich's confidential teleconference compromised by cell phone](#)
[Bruce R Koball](#)
- [Fired Contractor Arrested in Computer Sabotage](#)
[PGN](#)
- [Babbage-Catch Dolls?](#)
[PGN](#)
- [Web Spoofing Is No Joke](#)
[Edupage](#)
- [Computer threatens 11000 car-owners in Finland](#)
[Toomas Tamm](#)
- [Run For Your Lives! Beepers Go Berserk, Refuse to be Silenced](#)
[Norm deCarteret](#)
- [Double bills from SNDSS hotel](#)
[PGN](#)
- [Defense Science Board Task Force on Information Warfare -- Defense](#)
[A Blyth](#)
- [InfoWar \(a\)--fraud & scavenging](#)
[Mich Kabay](#)
- [Infowar \(b\): Misrepresentation on the Net](#)
[Mich Kabay](#)

- [New US regs ban downloadable data-security software](#)
[Lucky Green](#)
 - [Y2K problems? What about 1997 problems for Coast Guard? \[identity withheld\]](#)
 - [British Telecom plan for Y2K noncompliance fines](#)
[Lloyd Wood](#)
 - [Re: VISA fines banks with Y2K problems](#)
[Lloyd Wood](#)
 - [Denied removal from a data collection service](#)
[Dennis Glatting](#)
 - [Internet Archive - copyright violations and future embarrassment](#)
[Tim Slagle](#)
 - [7th Conference on Computers, Freedom, and Privacy](#)
[Bruce R Koball](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ **Newt Gingrich's confidential teleconference compromised by cell phone**

Bruce R Koball <bkoball@well.com>

Fri, 10 Jan 1997 14:53:30 -0800 (PST)

The New York Times reports today (10 Jan 1997) that Newt Gingrich was overheard in a telephone conference call to other House bigwigs on 21 Dec 1996 plotting strategy on how to deal with his ethics problems and possible attacks from opponents. This despite his promise, made the same day to the ethics subcommittee by his lawyer, that he would not use his office or his allies to orchestrate a counter-attack to the charges.

Big deal, you say? Politics as usual, you say?

I agree, except for one hook... the call was intercepted by a Florida couple on a scanner radio, most probably from the cell phone connection

of one of the participants. No fans of Newt, the couple reportedly recorded the conversation and passed it along to an anonymous Democratic Congressman, who released it to *The Times*.

Some people never learn... and therein lie the RISKS...

✶ Fired Contractor Arrested in Computer Sabotage

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

Thu, 9 Jan 97 10:15:08 PST

David Salas, 34, worked last summer as a subcontractor on the development of a computer system for the California Department of Information Technology. He was fired after falling out with his business partner. He has now been arrested on three felony charges, for ``allegedly trying to destroy'' the system. He is suspected of having built a backdoor into the system so that he could access it remotely. [Source: *San Francisco Chronicle*, 9 Jan 1997, although the article is very short on details.]

✶ Babbage-Catch Dolls?

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

Thu, 9 Jan 97 10:39:21 PST

Gears and relays of old-time mechanical computers have been known to inadvertently engulf various foreign objects, but Cabbage Patch

Snack Time

Kid dolls are designed to eat plastic food. These dolls were reportedly trying to ingest assorted children's hair and fingers during the recent holiday season, incurring some minor scrapes and bruises.

[Source: *San

Francisco Chronicle*, 31 Dec 1995, A2.] Mattel is offering \$40 to anyone

who returns a doll, according to an item I heard on the radio. Although

this risk has no direct computer-related connection, the absence of an

easily accessible off-switch does seem like a flaw in the design of the

human-doll interface. On the other hand, the existence of a reverse-flow

switch would probably be a bad influence on the eating habits of small children.

Always look a gift doll in the mouth, but don't look too closely.

The doll might have a ball, and it might be your (eye)ball.

🔥 Web Spoofing Is No Joke (Edupage, 9 January 1997)

Edupage Editors <educom@elanor.oit.unc.edu>

Thu, 9 Jan 1997 18:00:43 -0500 (EST)

Researchers at Princeton University have released a paper documenting ways that nefarious crackers could dupe unwitting Web browsers into divulging personal information, such as bank personal identification numbers or credit card numbers. One way to do this is to break into a legitimate Web server and alter the links to other sites, so that when users click to transfer,

they're actually transported to the cracker's computer where the virtual hijacker can watch every move they make (such as entering credit card info when prompted). The researchers suggest that Web surfers take the following precautions: disabling JavaScript in their Web browsing software; keeping an eye on the software's location line, to ensure they know where they are; and paying close attention to the addresses they visit. (*Chronicle of Higher Education*, 10 Jan 1997, A25)
<<http://www.cs.princeton.edu/sip/pub/spoofing.html> >

✶ Computer threatens 11,000 car-owners in Finland

Toomas Tamm <toomas@chem.helsinki.fi>
Fri, 10 Jan 1997 10:13:15 +0200 (EET)

In the Finnish TV news on 9 Jan 1997, it was reported that the Finnish car registry had sent mail to 11 thousand car-owners stating that the registration of their cars would be dropped from the registry, "because the car has been out of use". The registry representative said this was caused by a "computer error" the exact cause of which is being investigated. The registry then sent out 11,000 apologetic letters.

What if the program had silently marked the 11,000 registration records as expired?

Toomas Tamm, Department of Chemistry, FIN-00014 University of Helsinki FINLAND
toomas@chem.helsinki.fi +358+9-191-40173 <http://www.chem.helsinki.fi/~toomas/>

[Also reported by Jouko Holopainen <jouko.holopainen@xnet.otm.fi>. PGN]

⚡ Run For Your Lives! Beepers Go Berserk, Refuse to be Silenced

"Norm deCarteret" <nsdec@VNET.IBM.COM>

Fri, 10 Jan 97 08:56:25 EST

Today's front page of the *Wall Street Journal* hints of the apocalypse: ``A technical problem on the Skytel paging network led to a nationwide bout of beeper madness, as a digital deluge of erroneous call-me-back messages swept over more than 100,000 unwitting pager customers.''

What happened was an erroneous broadcast at 8 AM EST to over 100,000 Skytel pager customers, most of whom assumed it to be a local phone#. Thousands tried to return the call. The incident was then compounded by some 36 users who recognized the number for what it was, a PIN. They dialed Skytel, entered the PIN and their own phone numbers. ``The Skytel system then efficiently zapped those real phone numbers out: to the same 100,000 pager customers. Ever eager, thousands of them then returned calls to the diligent three dozen'' who got 300 calls an hour or more, still 40 an hour in the afternoon.

At one time or another, we've all been grateful to a helpful customer service rep who has managed to overcome ``the system'' and correct some problem plaguing us. Evidently, that's exactly what a Skytel

staffer was trying to do for a customer who wanted her pager service activated. But somehow ``a terribly wrong PIN'' was assigned, one that was linked to to a secret code Skytel uses to broadcast news to 100,000 users. The network computer saw the PIN was wrongly linked and rejected it, ``but the Skytel staff successfully overcame the computers recalcitrance'' and then tested the new customer's PIN by zapping the 7-digit number over the network so it would show up on her display. Scott Hamilton, Mtel (Skytels parent company) spokesman: ``with any kind of computer system, from time to time, numbers have to be jiggled, and they were attempting to jiggle. It was just a mistake.''

Who of us hasn't ``jiggled'' a computer or been profusely grateful to someone who did it for us and solved some nasty problem. One RISK is that many people who have to work with computers "know" how dumb they really are and have found end-around plays in order to get the job done. But, of course, sometimes the computer 'recalcitrance' is deliberate.

Norm deCarteret

[Also noted by Scott Call <scall@ccnet.com> and George C. Kaplan <gckaplan@cea.berkeley.edu>. PGN]

⚡ Double bills from SNDSS hotel

"Peter G. Neumann" <neumann@csl.sri.com>
Wed, 8 Jan 97 8:49:46 PST

Don't duck bill analysis for reservations made on 17 Dec 1996 at the San Diego Princess -- for example, for attending SNDSS on 10-11 Feb 1997 (see [RISKS-18.20](#)). ALL CHARGED DEPOSITS on that day were double billed because of a human/computer screwup. (However, you may duck billed platypuses while in San Diego.)

Defense Science Board Task Force on Information Warfare -- Defense

A Blyth <ablyth@easynet.co.uk>
Fri, 10 Jan 1997 21:04:55 +0000

A Defense Department panel, in an unusually strident report, recommended \$3 billion of additional spending over the next five years to improve the security of the nation's telecommunications and computing infrastructure. Warning of a possible "electronic Pearl Harbor," the task force appointed by the Defense Science Board also said the Pentagon should seek the legal authority to launch counterattacks against computer hackers. "There is a need for extraordinary action," the board's task force on "Information Warfare-Defense" stated in a report that was quietly released on Friday. Current practices and assumptions, it said, "are ingredients in a recipe for a national security disaster." The report also predicts that by the year 2005, attacks on U.S. information systems by terrorist groups, organized

criminals and foreign espionage agencies are likely to be
`widespread.'`

[The full article is entitled REPORT OF THE DEFENSE SCIENCE
BOARD TASK

FORCE ON INFORMATION WARFARE - DEFENSE (IW-D), By Thomas E.
Ricks, *The

Wall Street Journal*, 10 Jan 1997. PGN Excerpting. Also
contributed by

"Betty G. O'Hearn" <betty@infowar.com>. PGN]

InfoWar (a)--fraud & scavenging

"Mich Kabay [NCSA]" <75300.3232@CompuServe.COM>

10 Jan 97 16:45:17 EST

For RISKS participants struggling to convince their managers of
the
possibility of information warfare level II (inter-corporate
conflict via
information), here is a useful case.

Canada's Globe and Mail 97.01.10 pA1:

Letter drive linked to Shoppers employee: Owner of Meditrust
says he
believes campaign scared investors away from mail-order pharmacy.

By Jane Coutts and John Saunders, The Globe and Mail

A letter campaign attacking a mail-order pharmacy company has
been traced to

a mailbox rented by the secretary of a vice-president of
Shoppers Drug Mart.

The [C]\$11-a-month box is home to the Society of Concerned
Pharmacists,

whose listed address, Suite 142, 2671 Eglinton Ave. E., is in
fact Box 142

at Mail Boxes Etc., a private postal outlet.

Key points from the article:

- * No evidence yet of the legitimate existence of the SCP.
- * SCP accused of sending out 6,000 copies of a letter highly critical of the mail-order pharmacy business proposed by Meditrust Healthcare Inc.
- * Letter said SCP represented 6,000 pharmacists; now claimed to be typographical error (should have been 600 but no proof of any members at all).
- * Letter written by Larry Rosen, independent pharmacist partly funded in the past by Shoppers Drug Mart. . . .
- * ... but letter was signed by another person described as a practising pharmacist -- of whom the College of Pharmacists of Ontario has no record whatever.
- * Letter may account for failure of initial public offering of shares.
- * Private Investigator searched garbage of mail drop and found record showing that secretary rented box.

This minor case demonstrates the risks of (1) breaching authenticity by fraudulent misrepresentation; (2) the effects of breaches of integrity of data in the real world, including especially the investment community; and (3) the risks of breaches of confidentiality such as throwing out confidential information in plain garbage.

Extensions of these lessons to purely electronic data are clear: verify

authenticity and integrity of data before acting on any
information from
untrusted sources; obliterate data remnants. MEK

M.E. Kabay, Ph.D. / Director of Education National Computer
Security
Association <http://www.ncsa.com>

✂ Infowar (b): Misrepresentation on the Net

"Mich Kabay [NCSA]" <75300.3232@CompuServe.COM>
10 Jan 97 16:47:19 EST

Jack Kapica reports on cyberspace every Friday in *_The Globe and Mail_*. He points out today (Cyberia column, 97.01.10 p.A6) that despite the enthusiasm expressed by the likes of *_The Washington Post_*, *_The Economist_* and *_The New Yorker_*, AMAZON.COM does not, in fact, have more than 1,100,000 titles in stock as claimed. They actually have only 200 titles in stock in their warehouse. They just order the rest from distributors and wholesalers -- just like all other bookstores.

See <http://www.slate.com/features/amazon/amazon.asp>
for an article by Jonathan Chait and Stephen Glass.

Caveat lector.

M. E. Kabay, Ph.D. / Director of Education National Computer
Security
Association <http://www.ncsa.com>

✶ New US regs ban downloadable data-security software

Lucky Green <shamrock@netcom.com>

Tue, 31 Dec 1996 19:05:05 -0800

The new US crypto export regulations control the export of most if not all data-security software. Regardless if the software uses cryptography or not. Many software archives seem to be in violation of the new regs.

[Federal Register: December 30, 1996 (Volume 61, Number 251)]
[makes it illegal to export without a license:]

c.3. ``Software'' designed or modified to protect against malicious computer damage, e.g., viruses;

[For the full text, see
http://www.epic.org/crypto/export_controls/interim_regs_12_96.html]

This certainly controls virus checkers, firewalls, and other security software. There are substantial penalties involved in violating the EAR. The US can assess daily penalties and block all exports of a company's non-violating products. Criminal penalties apply as well.

"Export", as defined in the new regs, includes making software available on the web or via ftp.

If you have a virus checker or similar software available for ftp inside the US and the software can be downloaded from outside the US, you are most likely in violation of the new EAR which took effect on 12/30/1996.

If you do not wish to go to prison, you may want to consult an attorney immediately and remove all data security software from your server.

IANAL --Lucky Green <mailto:shamrock@netcom.com>

✶ Y2K problems? What about 1997 problems for Coast Guard?

<[identity withheld by request]>

Thu, 9 Jan 1997

On Wednesday 8 Jan 1997, the entire US Coast Guard discovered that its standard Spreadsheet no longer runs on Wednesdays (or Saturdays), and refuses to print files on Tuesdays and Thursdays! Mondays and Fridays are OK, though.

The Coast Guard uses a proprietary Operating System called CTOS, marketed by Unisys. Although most of the software was specifically built for the CTOS environment, some of it was ported over from other operating systems. A program called Ofis Spreadsheet is an amazing clone of Lotus 1-2-3 v2.2, for example.

On the above date, everyone noticed that their spreadsheet program no longer worked, giving what amounts to a Windows' General Protection Fault error at start-up. It turns out that the hexadecimal codes that CTOS uses to represent the date added an extra digit with the new year. Apparently, they went from FFFFFFFF to 10000000 at some point after New Year's Day. Unfortunately, some of the non-native applications (the 1-2-3

clone and the Progress db's seem to be the ones in question) can't handle this change elegantly.

Interestingly, although no word has yet been spread on how to solve the anecdotal Progress problems (of which I've seen no sign myself), the solution to the spreadsheet conundrum is to change the date format. Even though the spreadsheet file may not access any date functions, the application **does**, and it doesn't like MM/DD/YY formats from 1997 onwards. But if you change the startup files to indicate a DD/MM/YY format, the problem goes away...

RISKS: You may be concentrating on a problem (Y2K, which is a major effort in the Coast Guard just now) that is not **quite** as timely as another that is sneaking up on you. Watch out! This sort of embarrassment just might undermine your Y2K efforts.

Perhaps, from this time forward, it might be smart to run test systems with clocks set a month or more ahead of schedule. Just in case. I know that I will be.

British Telecom plan for Y2K noncompliance fines

Lloyd Wood <L.Wood@surrey.ac.uk>
Thu, 9 Jan 1997 18:24:32 +0000 (GMT)

BT recently merged with MCI to form Concert; will MCI be

following suit? Is the 18-week grace period long enough for previously complacent suppliers to rectify their systems? [**Electronic Telegraph**, City News, 9 January 1997]

[The 'red card' references are to a game called football, played here in the UK, where a red card signifies that a player is sent off

the pitch for an offence such as kneecapping an opponent or beating

up a spectator. This game has nothing whatsoever to do with American

football or Australian-rules football, and is **not** called soccer. L.]

<URL:<http://www.telegraph.co.uk:80/et?ac=000111464113065&pg=/et/97/1/9/cbt09.html>>

includes links to related resources and previous articles on the millennium

bug.

BT IN 'RED CARD' ALERT TO SUPPLIERS OVER 2000

By Roland Gribben

BRITISH Telecom is warning suppliers that they will be shown the ``red

card'' and be sacked if they cannot produce evidence that they are working

to change their computer and information technology systems to cope with the

year 2000 date change. The group has written to its 1,800 suppliers and

drawn up a green, amber and red coding system to detail the state of

preparedness. ``Red'' suppliers are in danger of being removed from the

list of suppliers.

More than half BT's suppliers have yet to answer inquiries about the change,

according to the latest edition of Computer Weekly. Milli Lewis, BT's year

2000 project manager, said: ``We are starting an escalation process which will leading to BT not trading with suppliers after an 18-week warning.``
BT has already started planning for changes in its computer network and aims to have everything in place by the end of next year, but along with other major groups also deeply involved in the exercise, it is worried that other companies down the supply chain will not be ready.

The telecommunications group is ready to step up the pressure on suppliers it feels are failing to demonstrate they are taking the change seriously and could start weeding out the laggards by March. It has a team of managers available to help companies tackle the problem.

<URL:<http://www.sat-net.com/L.Wood/>><L.Wood@ieee.org>+44-1483-300800x3435

✉ Re: VISA fines banks with Y2K problems (Wood, [RISKS-18.73](#))

Lloyd Wood <L.Wood@surrey.ac.uk>
Wed, 8 Jan 1997 15:06:50 +0000 (GMT)

In response, Michael C Voorhis wrote,

> Actually, it appears, you don't need to register in order to use that URL.

> It already has my "user code" attached to it.

><http://www.the-times.co.uk/news/pages/tim/97/01/06/timbizbiz01012.html?1297596>

> The correct URL for the web page is included above, everything to the

> right of the question-mark in the URL above specifies that I'm reading

> the article I would imagine.

>

> Hmm. I suppose as a RISKS reader I might have checked this, but I did not.

> A risk associated with passing URL's to other people, via e-mail?

Good question. Other people can now pretend to be you to the site, and browse the site without registering, giving false reading preference information to the site.

This is arguably good for web users as a whole, many of whom dislike having their preferences tracked, but bad for the content provider and for the user allocated the URL if the URL owner attempts to do customised profiling, page output or secure transactions based on the supplied data.

The registration could be made more secure, with name and password required each time for access instead of a bookmarkable identifier-in-URL - but many sites have gone away from that model, since it discourages casual use.

Here in the UK, the Electronic Telegraph, which I'm more familiar with, uses a similar identifier-in-cgi-for-state-machine URL.

<URL:<http://www.telegraph.co.uk/>>

They've completely redone their identifier system, requiring that people reregister, three times since going online in 1994, presumably due to running out of allocation numbers (new URLs are considerably longer) and/or wanting to purge 'old' users from their database.

I don't know what data is generated or how the ET plans to move to a payment

system for searching their archives, which have been on a 'free trial' basis for the last couple of years.

Open, easily-subverted registration systems like these provide a risk to the overall quality of the provider's tracking data and a risk to the individual registered, but it's probably an acceptable risk to society as a whole, IMO, since it's convenient and makes the content referrable.

For the user so inclined, it's a great way of increasing your privacy by providing inaccurate data and fudging the data generated to track your reading interest.

Anyway, when you registered the only true information you provided was a valid e-mail address for automatic verification - right? The online newspapers are starting from a mass of unverified information, and the tracking information can't make it any better. Entropy goes one way, and (in this case) I can't see the ET easily moving to a payments model for their search engine any time soon.

<URL:<http://www.sat-net.com/L.Wood/>><L.Wood@ieee.org>+44-1483-300800x3435

⚡ Denied removal from a data collection service

Dennis Glatting <dennis.glatting@plaintalk.bellevue.wa.us>
Fri, 3 Jan 97 08:44:04 -0800

Recently, there was a message posted in this forum of data

collection
services and a list contacts to have yourself removed from them.
I contacted
several of those services and was surprised by the response from
Bigfoot. Apparently, their database is one-way although I can
subscribe to
their service and *modify* my profile.

> From: Admin@Bigfoot.com (Bigfoot Admin)
> Subject: Re: REMOVE
> Date: Fri, 03 Jan 1997 09:08:26 -0500
>

...

> Currently, we can not delete listings that have already been
> entered in our database. However, you may edit your profile to
> become unlisted and therefore have no information visible to
> anyone searching for you on our directory. Just follow the
> following steps to change your status:

I do not know how Bigfoot collected my e-mail addresses (they
have collected
both past and present e-mail addresses) but spammers tend to
collect
addresses by scanning the USENET. To battle the onslaught of
spam I no
longer use a valid return address in my news postings. I wish
that were not
necessary.

The risks? First, unknown to the people, companies collect
information on
them and freely advertise it. Imagine the repercussions of
battered women
hiding from their spouse. Two, you may or may not have any
rights regarding
the information about you they make available. Lastly, to
protect ourselves
we are being forced into an anonymous society.

-dpg

🔥 Internet Archive - copyright violations and future embarrassment

Tim Slagle <slagle@drip.Colorado.EDU>

Tue, 7 Jan 97 15:08:14 -0700

I was looking through the logs of our HTTP server and saw a large block of accesses from widener.archive.org. It looked like they were sequentially downloading each page on our server, but I didn't recognize the address as being one of usual search services.

I checked out their web site (www.archive.org) and it looks like they are systematically making and storing copies of everything they can access over the Internet. Their pages talk about what a great research tool their database will be for future 'net historians, but also says that it will be a treasure-trove for marketers and entrepreneurs.

I didn't find a discussion of their position on the copyright issues their project brings up, but I doubt that whole-scale copying of entire sites without any human intervention or commentary is 'fair use', especially considering the American Geophysical Union v. Texaco case ([RISKS 16.68](#)). At more than 1 TB of text and images copied off of the 'net (and 100GB more each week), they could have the largest archive of violated copyrights in the world.

Giving them the benefit of the doubt (that they aren't maliciously copying other people's work for profit), a risk is that one's enthusiasm for a new

medium or technology can blind one to the existing legal guidelines that apply to one's project. I don't really have the interest or resources to pursue an infringement suit, but I bet someone else (like an artist, publisher, or software company) will, especially if the Internet Archive starts allowing access to their data.

Another risk for people with Web pages is that every rant or embarrassing picture that you publish on the Web (and later think better of and remove) could now be accessed by future generations without your control. It could be argued that posting to Usenet implies a certain loss of rights to control the fate of your message, given the nature of Usenet distribution. I wouldn't think the same is true for Web pages (but I have no qualifications in IP law).

Tim Slagle, slagle@colorado.edu, <http://optics.colorado.edu/~slagle>

✶ 7th Conference on Computers, Freedom, and Privacy

Bruce R Koball <bkoball@well.com>
Wed, 8 Jan 1997 18:12:41 -0800 (PST)

The Seventh Conference on Computers, Freedom, and Privacy
CFP'97 : Commerce & Community, 11-14 March 1997
San Francisco Airport Hyatt Regency; Burlingame, California

CFP'97 will assemble experts, advocates, and interested people from a broad spectrum of disciplines and backgrounds in a balanced public

forum to address the impact of new technologies on society. This year's theme addresses two of the main drivers of social and technological transformation: How is private enterprise changing cyberspace? How are traditional and virtual communities reacting?

Topics in the wide-ranging main-track program will include:

- Perspectives on Controversial Speech
- The Commercial Development of the Net
- Governmental & Social Implications of Digital Money
- International Perspectives on Cryptography
- Cyberpunks & Cybercops
- Regulation of ISPs
- Spamming
- Infowar
- Intellectual Property and Info-Property
- The 1996 Elections: Creating a New Democracy
- The Coming Collapse of the Net

In addition, there will be parallel-track lunch-time workshops:

The Case Against Privacy	How a Skiptracer Operates
Cyberbanking	How the Architecture
Regulates	
Rights in Avatar Cyberspace	National I.D. Cards
Public Key Infrastructures	European IP Law
Sexual Harassment in Cyberspace	Virtual Communities
Domain Names	Archives, Indexes & Privacy
Government Regulation of E-cash	Crypto and the 1st Amendment

and tutorials:

- The Economics of the Internet
- Regulation of Internet Service Providers
- The Latest in Cryptography
- The Constitution in Cyberspace
- Info War: The Day After
- Personal Information and Advertising on the Net
- Transborder Data Flows and the Coming European Union
- Intellectual Property Rights on the Net: A Primer

A complete conference brochure and registration information are available on our web site at: <http://www.cfp.org>

For an ASCII version of the conference brochure and registration information, send e-mail to: cfpinfo@cfp.org

For additional information or questions, call: 415-548-2424



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 18: Issue 76

Thursday 16 January 1997

Contents

- [Taco Bell-issimo](#)
[Peter G. Neumann](#)
- [Telstar 401 catastrophic failure](#)
[Lauren Weinstein](#)
- [More on fired contractor arrested in computer sabotage](#)
[Cathy Horiuchi](#)
- [Five-Million-Dollar Bug](#)
[David Kennedy](#)
- [Redundant virtual circuits lead to single point of failure](#)
[Sidney Markowitz](#)
- [Missing-characters file: Not the only ones with that problem](#)
[Mark Brader](#)
- [Electronic airline ticketing](#)
[Robin Burke](#)
- [More Y2K humor: Split the difference](#)
[Mark Brader](#)
- [Re: April 1 considered harmful](#)
[Chuq Von Rospach](#)
- [Problem with Insight's WWW mail](#)
[Christopher G. Holmes](#)

- [Risks of miskeying e-mail addresses](#)
[Gerard A. Joseph](#)
 - [Congress and FBI aided Gingrich's cell-call snoops](#)
[Jim Warren](#)
 - [FBI Offers New Proposal for Digital Wiretaps](#)
[Edupage](#)
 - [Re: New US regs ban downloadable data-security software](#)
[David Holland](#)
 - [FreeWare WORD macro antivirus release: PC/MAC](#)
[Padgett Peterson](#)
 - [DIAC '97, Seattle 1-2 March 1997](#)
[Susan Evoy](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ Taco Bell-issimo

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

Wed, 15 Jan 1997 17:07:30 PST

Willis Robinson, 22, of Libertytown, Maryland, was sentenced to 10 years in prison (6 of which were suspended) for having reprogrammed his Taco Bell drive-up-window cash register -- causing it to ring up each \$2.99 item internally as a 1-cent item, so that he could pocket \$2.98 each time. He amassed \$3600 before he was caught. [AP item in the *San Francisco Chronicle*, 11 Jan 1997, All, pointed out to me by Glenn Story.] This is another version of the old salami attack.

⚡ Telstar 401 catastrophic failure

Lauren Weinstein <lauren@vortex.com>

Mon, 13 Jan 1997 16:46 PST

On Saturday morning, 11 Jan 1997, AT&T's Telstar 401 satellite, with a full complement of both C and Ku band transponders, went dead. Technicians have been unable to reestablish any contact. The satellite normally carries both broadcast network and syndicated television programming. The networks, as "platinum" customers, were quickly switched to an alternative bird. Almost everyone else has been scrambling to find transponder space for their programming.

The risk? Don't assume the satellite will always be there!

--Lauren-- Moderator, PRIVACY Forum www.vortex.com

✶ More on fired contractor arrested in computer sabotage **(RISKS-18.75)**

Cathy Horiuchi <cathy.horiuchi@smud.org>

Thu, 16 Jan 1997 11:05:00 PST

This was reported locally in the **Sacramento Bee**, 8 Jan 1997, and is being discussed extensively if informally hereabouts. Unfortunately, the twenty-column-inch long article is not stored at www.sacbee.com's archive page online.

The accused saboteur was a subcontractor of a subcontractor of a contractor of a state agency. He spent at least six hours online before being

detected, and then crashed the system, which had to be restored from backup.

The newspaper article states damages as limited to \$10,000, but that number

may be invalid. Here in Sacramento the cost of a first-rate security

incident audit by an outside firm runs \$20 to \$30K, plus the cost of system

changes based on security weaknesses.

The nature of professional services procurement in government lends itself

to multiple levels of subcontracting. Most computer technical experts do

not work independently, since that would require large insurance bonds and

skills writing responses to governmental requests for proposal. Often

contracting and outsourcing firms bid for contracts, and only hire

contractors once the bid is rewarded, so there is constant staffing churn.

The RISK here is starkly stated in the article, in the last few paragraphs,

where the opinions of the management team are given: "Department officials

claim they did not know Salas was fired because he was a subcontractor and

they had no direct dealings with him. John Thomas Flynn, who heads the

department, said his staff did everything 'by the book'....

Flynn said, 'We

didn't drop our guard.' Since the intrusion, computer security has been

improved. But even without the extra precautions, it is unlikely that such

an intrusion will ever occur again, department officials said."

Isn't it the job of management to know and manage the chain of control?

Even if a department employee were tasked with managing all the contractors,

there is a big difference between knowing a contractor is working between 8 & 5 and knowing exactly what that person is doing and creating. Traditional management practice does not require or expect technical knowledge. That means security, reliability, auditability are dependent on the integrity of the technical workforce, not on the management and quality control processes.

The idea that it cannot happen again is naive; the statement itself is an attractive nuisance. No system is static in this day and age. The next DNS server or Internet firewall that is installed will create a situation wherein this may happen again, since it appears, from what has been stated in public, management has learned little from the event.

Cathy Horiuchi, Principal IT Analyst, Sacramento Municipal Utility District
choriuc@smud.org

Five-Million-Dollar Bug

David Kennedy <76702.3557@CompuServe.COM>
10 Jan 1997 18:30:22 EST

[DMK: Many of us can remember the \$6 Million Man, well....]

Electronic Roach Implants Probed, By ERIC TALMADGE
Courtesy of Associated Press via America Online's News Profiles:

A big brown cockroach crawls across the table in the laboratory of Japan's most prestigious university. The researcher eyes it nervously, but he

doesn't go for the bug spray. He grabs the remote. This is no ordinary under-the-refrigerator-type bug. This roach has been surgically implanted with a micro-robotic backpack that allows researchers to control its movements. This is Robo-roach. ...

[With a \$5 million dollar grant from the Japanese Government -- no Proxmires in the Diet obviously]

Professor Isao Shimoyama, head of the bio-robot research team at Tokyo University says, electronically controlled insects carrying mini-cameras or other sensory devices could be used for a variety of sensitive missions -- like crawling through earthquake rubble to search for victims, or slipping under doors on espionage surveillance. ...

The controls, however, still have a few serious bugs of their own.

Swiss researcher Raphael Holzer, part of the Tokyo University team Holzer jolts a roach with an electric pulse to make it move slightly to the right and keep to an inch-wide path. Instead, the roach races off the edge of a table into Holzer's outstretched hands.

``The placement of the electrodes is still very inexact,'' he admits, setting the bug back on track. ...

Holzer is optimistic. ``The technology isn't so difficult,'' he said. ``The difficulty is to really understand what is happening in the nervous system.''

✶ Redundant virtual circuits lead to single point of failure

Sidney Markowitz <sidney@research.apple.com>

Tue, 14 Jan 1997 10:48:45 -0800

This note from Finland was passed on to me by a friend. It points out the Risks of working with virtual systems while carrying assumptions and habits from the real (physical) world.

... we had here data line breakdown last week and no Internet connections worked. It happened so that there was heavy icing on the line between Oulu and Kajaani which caused the break.. we had reserve line but that was also broken.. that line was leased from Finnet and it happened that as logically separate it was physically that same line which Finnet had leased from the primary operator! The agreement with Finnet was ended immediately.

Sidney Markowitz <sidney@research.apple.com>, Virtual Rocket Scientist
Apple Research Labs, Apple Computer

*fh ARPAnet loses New England despite 7-trunk ``redundancy'';
one accidental
cable cut in White Plains knocks out all 7 links, 12Dec86 (S 12
1)

[Long-time RISKS readers will recall the event on 12 Dec 1986
([RISKS-4.30](#))

when New England was completely cut off from the ARPAnet because a single cable that was accidentally severed in White Plains, New York, happened to contain all seven trunk lines that had been established to provide

physical redundancy! Several other similar cases are also in the RISKS archives, including the backhoe in Annandale VA that on 14 Jun 1991 took out two *separate* cables ([RISKS-11.92](#)). Physical, schmysical; but, is it perfectly logical? PGN]

✂ Missing-characters file: Not the only ones with that problem

Mark Brader <msb@sq.com>

Wed, 15 Jan 1997 04:39:08 EST

A *Houston Chronicle* article by Dwight Silverman was forwarded to comp.dcom.telecom by Tad Cook a few weeks ago. It was about various changes that Southwestern Bell, the phone company there, is planning to make in their directories.

One of the changes is that they plan to list e-mail and WWW addresses for businesses that want to supply them. However, this will not be possible for residential listings at first -- I swear, this is just how the posting appeared -- because

```
# "Right now we have a certain system constraint in our
residential
# listings database that prevents us from printing certain
characters on
# a page," Hillyer said. "The biggest problem is that we can't
print the
# sign."
#
# The sign is a crucial part of all e-mail addresses,
separating the
```

```
# user's name from the computer system -- or domain -- he uses.  
--  
Mark Brader, msb@sq.com           "But I do't have a ' ' key o my  
termial."  
SoftQuad Inc., Toronto           -- Ly  
[nn] Gold
```

[Southwestern Bell evidently needs a noncommercial source for obtaining its commercial-at (@) characters.

⚡ Electronic airline ticketing

Robin Burke <burke@cs.uchicago.edu>
Mon, 13 Jan 1997 11:09:26 -0600 (CST)

I have had recent and vivid evidence of the risks of much-hyped "electronic ticketing" systems for air travel. My wife called to confirm her reservation on a return flight, only to discover that, according to the airline she had already flown a week earlier. "You've used that ticket," she was told. Since electronic ticketing procedures require that the agent match the user's ID with the ticket information, she was treated like someone trying to scam the airline by flying twice.

Fortunately, the date of usage was different than the date for which the ticket was issued, although the flight number was the same, and she had various records, such as her credit card receipts, through which to assert her identity, but only after many hours on the phone.

The supervisor who finally resolved her case seems to be handling a lot of

electronic ticketing problems. The agent is supposed to look at the passenger's ID, and pull up the ticket record corresponding to that traveler. However, there is also a receipt for the electronic ticket: "not valid for travel" that has the name and ticket number on it. Apparently, in this case, the gate agent used the ticket number from the receipt, but typed it in wrong, then failed to notice that the ticket record retrieved was for a different passenger than the one named on the receipt.

No record is made of the validating transaction (the agent matching the ID against the ticket record), except for the agent marking the record as used, so the airline has no way of knowing who actually traveled on our ticket, and we had no way, within the system, of documenting the fact that the ticket had been used by someone else.

I, for one, will stick with a physical ticket.

Robin University of Chicago, Computer Science Department
<http://www.cs.uchicago.edu/~burke/>

⚡ More Y2K humor: Split the difference

Mark Brader <msb@sq.com>
Tue, 14 Jan 1997 17:54:22 GMT

In comp.software.year-2000, Darren Berar suggests a compromise for those struggling with converting from 2-digit to 4-digit years.

| I suggest the 3 digit year. It puts the whole issue off for

another

| 1000 years and is only 50% of the work to implement a 4 digit year. :-)

Mark Brader

"Should array indices start at 0 or 1?

My ecumenical

msb@sq.com

compromise of 0.5 was rejected

without, I thought,

SoftQuad Inc., Toronto

proper consideration."

-- Stan

Kelly-Bootle

[Mark noted that there were two follow-ups (follows-up?) in that

newsgroup from people who took this message seriously!

Incidentally,

the 1996/2001 edition of the annual Denning Newsletter from Peter and

Dorothy Denning -- which this time looks back from the future in 2001 --

indicates that the Y2K problem will have been successfully postponed for

another 48 years by observing that K is properly equal to 1024, so that

COBOL programmers could simply change the representation of the year field

from base 10 to base 2. Verrry cute. Happy New Year 2000 to the Dennings

for that one. PGN]

✉ Re: April 1 considered harmful (Evans, [RISKS-18.74](#))

Chuq Von Rospach <chuqui@plaidworks.com>

Sun, 12 Jan 1997 13:03:14 -0800

>We need to address the risks involved in even having a 1 April in the

>calendar. What if a powerful newbie takes a 1 April prank seriously, and

>dives in to "fix" something? What are the risks there?

Shrug. Christmas offends non-Christians. Should we do away with it?

Halloween has satanic roots (according to some; it's actually pagan. Not everyone sees the difference).

No offense intended to William Evans, but this seems to me to be well-intentioned but creeping PC-ism. Someone might interpret an April fools joke wrongly. Therefore, do away with April fools. Someone might drink, drive and kill someone in a car. Obviously, do away with drinking and driving.

Personally, I'd go for the cars first. They kill a lot more people than April Fools jokes do. I think we need to keep perspective. Just because there *is* a risk doesn't necessarily mean we have to obliterate anything that causes a risk.

Life is not about removing risks. Life is about understanding and managing risks, and resolving SERIOUS risks. Just because something might be a problem doesn't mean it is, or is worth fixing....

Now, having said that, folks who pull stunts like this (not that I'd know anyone who has, not me. nope) have a responsibility to do so in a non-destructive manner. It's sort of like drinking and driving -- it's not the drinking that's the problem, it's the idiot who doesn't know enough not to drive drunk. A good April Fools joke merely causes embarrassment when someone falls for it. That's half the fun of designing those things. If they cause damage by design or accident, then the writer of the joke ought

to be responsible for the impact of it. Doesn't matter if you meant to throw a firecracker at someone or not, if you blow off a finger, "I didn't mean to" isn't a valid defense...

I think this piece brings up an interesting meta-question: the risk of RISKS: by focusing on risks in this forum, do we run the risk of losing perspective on risk? Because if we are just as seriously talking about doing away with April 1 over the risks of a misplayed joke as we are bugs in air traffic control systems and the risks to human life, then we sure have lost our sense of perspective. All risk is not created equal, and sometimes we seem to forget that...

Chuq Von Rospach (chuq@solutions.apple.com) Software Gnome
Apple Server Marketing Webmaster <<http://www.solutions.apple.com/>>

[NOTE: This message is from the unidentified creator of one of the best April-Fools spoofs ever: the SPAFFORD SPOOF, [RISKS-6.52](#), 1 Apr 1988, and a follow-up from Spaf in [RISKS-6.54](#). PGN] [typo corrected in archive]

⚡ Problem with Insight's WWW mail

Christopher G. Holmes <holmes@papillonres.com>
Thu, 16 Jan 97 15:23:00 EST

I just discovered a problem with Insight's new WWW based on-line purchasing system. Insight sells personal computers & peripherals.

When purchasing an item, the system asks you to set up an account first.

Setting up an account is simply filling in a form with name, address, and phone #. An account # is then assigned.

A coworker set up an account with them a few weeks ago and bought something for his personal use, though he gave the office phone #. I set up an account a few days ago to buy something for work and gave the same office phone #. The system gave me the coworker's account #, but gave no indication that this was an existing account. All information needs to be entered again at "check-out" in addition to supplying a credit card # & shipping address.

I received my order today with my coworker's name & home address on the bill. I called and explained the situation. The service rep told me that account #'s are keyed to the phone #. She checked and told me that the proper credit card had been billed, but that the credit card co. had not checked the order for a correct billing address, etc. (This check is pretty standard for mail order these days. In fact, most outfits will only ship to the CC billing address). So no harm done, but I had a hard time convincing the rep that this was a problem that needed to be addressed. I can imagine a scenario where a someone's home address is given to some jerk in the same office who's been harassing him/her. And what if my phone # changes? And the old number is reassigned? The phone # is also used as a "password" to help verify the account # when checking

order status. Will we never learn?

Christopher Holmes

✦ Risks of miskeying e-mail addresses

"Gerard A. Joseph" <gerard@ozemail.com.au>

Thu, 02 Jan 1997 10:45:01 -0800

Most users have learned at least once that a computer will do what it's told, even if it's not what the user intended (provided the input is valid).

It would appear that many users are careless about handling and entering e-mail addresses. If such carelessness results in an invalid e-mail address, no real harm is done; the originating user will probably get a message back to that effect, realize his error, and resend the message with the destination address duly corrected.

However, an error that results in a valid e-mail address has potentially more serious consequences. It can result in a significant and embarrassing breach of privacy, and, depending on the honesty and the diligence of the unintended receiver, may remain unknown to the sender until it surfaces through some other means. I often receive misaddressed e-mail, some of it intensely private in nature. While courtesy and common sense dictate that I return it promptly to the sender and inform him of the error, nothing about the Internet can guarantee the sender that any private information he

unintentionally disclosed to me will not be abused.

E-mail addresses, like telephone numbers, can be wrongly transcribed or miskeyed. With a burgeoning user population, it would seem that there is an increasing probability that a randomly miskeyed e-mail address will actually be someone else's e-mail address. Users should develop an awareness of the risks to their privacy (as well as to the effectiveness of their communication!) of getting e-mail addresses wrong.

✶ Congress and FBI aided Gingrich's cell-call snoops (Re: [RISKS-18.75](#))

Jim Warren <jwarren@well.com>
Wed, 15 Jan 1997 17:09:31 -0800

Please note that it is the U.S. Congress that aided the cell-phone industry's initially remaining unsecure by making it unlawful to intercept calls that thus allowed cell peddlers to tell tech-naive prospects that cell calls were "safe".

But it is our federal enforcers -- led by the FBI -- who have zealously and diligently *BLOCKED* installation in U.S. cellphones of often-proposed, repeatedly-urged, readily-available automated scrambling technology to uncrackably protect the privacy of personal cell-phone calls, and also protect cell-phone id numbers -- that are *still* broadcast in the clear and thus trivially intercepted and cloned, costing the cell industry "billions"

of dollars (that is, *if* the folks using cloned fones would actually pay for the calls that they make for free).

My information is that our FBI even had a major hand, earlier this decade, in keeping the European cell-phone standards committee from finally adopting cell-phone standards that they ready to accept, that included automated uncrackable voice scrambling for *all* new cell phones.

Seems our FBI told the French security folks how awful that would be for government snoops (i.e., all cell-users must be considered potentially guilty of something), and the French instantly demanded that the call-security aspects of Euro cell-phone standards be trashed. They were.

Jim Warren

✶ FBI Offers New Proposal for Digital Wiretaps

Edupage Editors <educom@elanor.oit.unc.edu>

Thu, 16 Jan 1997 18:10:07 -0500 (EST)

The Federal Bureau of Investigation has released for public comment a new proposal for facilitating tapping of digital phone calls by law enforcement officials armed with court orders. Under the new proposal, which is significantly more modest than what the Bureau had asked for in a earlier plan, law enforcement officials would operate under a formula in which (for example) 523 phone lines could be monitored simultaneously in a place such as Manhattan. Privacy advocates oppose the FBI's plan as an

unacceptable

expansion of electronic surveillance. (*The New York Times*, 15 Jan 1997, A8; Edupage, 16 January 1997)

✶ Re: New US regs ban downloadable data-security software ([RISKS-18.75](#))

David Holland <dholland@hcs.harvard.edu>

Thu, 16 Jan 1997 17:12:15 -0500 (EST)

"Lucky Green" (shamrock@netcom.com) wrote:

> [Federal Register: December 30, 1996 (Volume 61, Number 251)]
> [makes it illegal to export without a license:]
>
> c.3. ``Software'' designed or modified to protect against
malicious
> computer damage, e.g., viruses;
>
> [For the full text, see
> http://www.epic.org/crypto/export_controls/interim_regs_12_96.html]

The cited text is not to be found on that page. (Standard RISK...) I found it at <http://jya.com/ke121396.htm> using Altavista.

It does appear that the language in question appears in the list of controlled items, even though in most previous documents of this sort virtually identical language appears as an exception to export controls. Did somebody goof when preparing the new regulations?

In any event, it appears that later language

Note: 5D002 does not control:

a. ``Software'' required'' for the ``use'' of equipment

excluded

from control under the Note to 5A002.

b. ``Software'' providing any of the functions of equipment

excluded from control under the Note to 5A002.

exempts anything that uses encryption only for access control or uses only message digests. Since this describes most existing virus protection software, I think some major legal wrangling will be necessary.

Note that almost all system software is designed to protect against malicious computer damage; if legal wrangling results in such software in fact becoming subject to export control, most operating systems projects are going to have major problems.

David A. Holland

dholland@hcs.harvard.edu

✶ FreeWare WORD macro antivirus release (PC/MAC)

Padgett Osirus <padgett@gdi.net-antispam>

Wed, 15 Jan 1997 21:45:16 -0500

Many people said it could not be done, but that just gets me interested and after literally months of obsessive programming (fortunately do not need much sleep 8*) on 14th January I posted for release as FreeWare (no charge for non-commercial use): MacroList.

Like the WORD macro viruses, this defense is designed to work on both MAC and PC platforms and anything from a 386/SE 30 to Pentium Pro 200/Power PC 100.

A macro itself, it builds on the concept that some things in WORD are not subvertable by a document/template and provides a mechanism for detection of any abnormalities.

Like the rest of my programs, it has not a clue what a virus is, instead it gives users visibility into the areas where viruses reside and allows the user to decide what to do (DELETE ALL is an option).

I have designed it to be compatible with other anti-virus programs (even SCANPROT) though MacroList is effective even against E-Mail launches of encrypted messages.

Enough said: it may be downloaded from <http://www.netmind.com/~padgett/>

- select "AntiVirus Hobby" and coming soon to sites near you.

Warning: there is a message in the ABOUT.

[A. Padgett Peterson]

⚡ DIAC '97, Seattle 1-2 March 1997

Susan Evoy <sevoy@Sunnyside.COM>

Tue, 14 Jan 1997 11:09:26 -0800

Community Space & Cyberspace

What's the Connection?

<http://www.scn.org/tech/diac-97>

March 1 - 2, 1997, 9:00 am - 5:00 pm

University of Washington HUB

Seattle, WA USA

Will cyberspace destroy society by turning us all into high-tech couch potatoes? Or will it provide unprecedented opportunities for community involvement? On March 1 and 2, 1997, Computer Professionals for Social Responsibility (CPSR) will present its sixth DIAC ("Directions and Implications of Advanced Computing") conference to help answer those questions. The theme is "Community Space and Cyberspace: What's the Connection?" and our aim is to challenge some of the cyber-spacy hype and bring the discussion back to earth to the communities we live in.

Howard Rheingold, best-selling author of "The Virtual Community: Homesteading on the Electronic Frontier" will give the keynote address on March 1. Howard's presentation will be followed by panel discussions on economics, education, high-technology social mediation, and other topics. In these panels computer pioneers, activists, and other thinkers and doers will describe their experiences and ideas on what has changed, what may change, and, most importantly, what citizens can do to make the technology more responsive to community needs.

Some of the Panelists include (among others)

- + Peter van den Besselaar, Social Science Informatics, University of Amsterdam and De Digitale Stad (the Digital City), Amsterdam
- + Amy Borgstrom, Executive Director, ACENET, OH
- + Amy Bruckman, Researcher, MIT Media Lab, Cambridge, MA
- + Steve Cisler, Senior Librarian, Apple Computer, Cupertino, CA
- + Jamie McClelland, Libraries for the Future, New York, NY
- + Peter Miller, Network Director, Community Technology Center's Network (CTCNet), Newton, MA
- + Kevin Rocap, California State University at Long Beach

+ Roland Waters, CEO, RTIME, Inc.

The second day, March 2, will feature workshops on a variety of topics

presented by practitioners from the Pacific Northwest, Boston, Amsterdam, New York City, and many other places.

Workshop Topics include

- + Libraries in Cyberspace
- + Community Voice Mail for Homeless Clients
- + Networking for Non-Profits
- + City Government Programs On-Line
- + Telecommunications and Educational Reform
- + On-Line Services: Forum for Collaboration or Technology of Isolation?
- + Safety in Cyberspace
- + Civil Liberties in Cyberspace
- + Navigating the Maze of Telecommunications Policy Changes
- + ...

For more information: Doug Schuler, douglas@scn.org, 206.634.0752



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 18: Issue 77

Monday 20 January 1997

Contents

- [Playboy strikes again](#)
[PGN](#)
- [Potential misery in Missouri: Taxes For Telephiles](#)
[Mike Coleman](#)
- [Leaking WWW surfer interest profiles](#)
[Anders Andersson](#)
- [Re: Handwritten signatures used for verification](#)
[Dave Finkelstein](#)
- [Re: UPS use of handwritten signatures, Lauren Weinstein article](#)
[PGN](#)
- [Blaming the safety people](#)
[Joshua Levy](#)
- [The Millennium problem: another too-young case](#)
[David R. Vinograd](#)
- [Y2036, Y2038, and the superiority of UNIX](#)
[D.J. Bernstein](#)
- [Re: More Y2K humor: Split the difference](#)
[Tony Lauck](#)
- [Re: More on fired contractor...](#)
[Carlie Coats](#)

- [Re: Taco Bell-issimo](#)
[Vincent Weaver](#)
 - [IBMmail flame on -- albeit out of character](#)
[PGN](#)
 - [Re: Risks of miskeying e-mail addresses](#)
[Darin Johnson](#)
[Niall Murphy](#)
 - [Irrelevant risks of miskeying e-mail addresses](#)
[Lawrence H. Smith](#)
 - [Chuq spoofing Spaf, and the archives](#)
[Adam Shostack](#)
 - [Privacy Digests](#)
[PGN](#)
 - [The SEI Conference on Risk Management - Preliminary Program](#)
[Carol Biesecker](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ **Playboy strikes again**

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

Fri, 17 Jan 1997 9:25:52 PST

TCI's cable-TV provider in Springfield, Missouri, was testing its planned inclusion of the Playboy Channel (to begin in February), when the Cartoon Network channel suddenly began airing the Playboy video along with the regularly programmed Flintstones' audio. The results were perhaps more noticeable than they might have been, because bad weather had closed the local schools and children were at home. [Source: Associated Press item in the **San Francisco Chronicle**, 17 Jan 1997, AS2. Maybe the program was something about Sharon kissing the Barney Stone?]

There seems to be something magnetically RISKS-attractive about the Playboy Channel, which last summer appeared unscrambled in the Palo Alto area because of a power-failure-induced chip failure ([RISKS-18.50](#)). A PC program [a nicely overloaded acronym, since the program was presumably not politically correct!] had previously appeared in the *Jeopardy* time-slot in the Chicago area for 10 minutes, due to a screwup ([RISKS-18.22](#)). Of course, what comes around goes around; 10 years ago the Playboy Channel was intentionally disrupted by a CBN employee, with satellite-spoofed programming declaiming ``Repent Your Sins'' ([RISKS-10.62](#)).

✂ Potential misery in Missouri: Taxes For Telephiles

Mike Coleman <coleman@chez-gnu.cstp.umkc.edu>

Fri, 17 Jan 1997 17:43:51 -0600 (CST)

Being the technophile, or perhaps just temporarily insane, I decided to try filing my taxes using the IRS's and State of Missouri's "Telefile" system. These systems allow the user to key in the figures from a simple return on their touch-tone phone. The systems also compute several values and speak them back to the user so that said user can record them for future reference.

Observations:

1. Both systems provided my authentication information in an unsealed packet through the USPS, even though I had not requested this.

Ergo, it would be quite simple for someone else to file for me. Ugh. (Hmm, if I couldn't file because someone beat me to it, would that count as "Denial of Service"?)

2. Both systems use a number as a "user id". The IRS number seemed suitably mysterious, but the Missouri number was quite familiar, being of the form "ABACADADB". Familiar, that is, because that pattern is also a perfect match for my Social Security Number. Ugh.

3. The user-interface for the IRS system was nice enough, albeit somewhat tedious. The Missouri system, on the other hand, had the annoying habit of rattling off figures at unexpected moments without providing the rattled user a means for having them repeated. Ugh.

Each item seems to involve a poor solution to a problem that has superior solutions that are well-known and relatively simple.

Mike Coleman <http://ctr.cstp.umkc.edu/~coleman>

🔥 Leaking WWW surfer interest profiles

Anders Andersson <andersa@Mizar.DoCS.UU.SE>

Fri, 3 Jan 97 23:52:00 +0100

I notice that AltaVista's inline advertisements link to a server outside Digital, "ad.doubleclick.net", and that the URL includes the user's list of keywords being searched. I'm concerned that these URL's may

occasionally
leak information about the user's interests and inclinations to
third
parties, information which the user may prefer to keep private.

This is not a new problem that appeared with the inline ads,
since also the
Referer: field of the HTTP protocol discloses to a target server
exactly
what AltaVista index page led the user to it. However, this
requires that
the user willfully follows that link.

If sensitive information being leaked via the Referer: field is
a problem,
the user may obtain client software that withholds Referer:
data, either
conditionally or unconditionally. Also, a user who has asked
AltaVista for
"gay" pages is probably not too concerned about accidentally
disclosing this
fact to the maintainer of said "gay" pages.

However, the doubleclick.net ads appear to bear no relationship
to the
keywords being searched, and they appear not only in the URL for
the
hyperlink to follow, but also in the IMG SRC URL. This means
that in order
to avoid disclosing my keyword lists to doubleclick.net, I have
to disable
automatic loading of inline images when using AltaVista!

Why is it that when I perform a search for, say, "gay OR nazi AND
scientology", AltaVista tricks my browser to give this very
search string
away to an advertising company by means of an inline image (the
contents of
which has nothing to do with my search)? I think I can trust
the AltaVista
maintainers not to save my keyword lists for future analysis,
but what about
an advertising company?

It's kind of serendipity reversed. When you open a book to look up information on a specific subject, the book scans your mind to find out what other interests and hobbies you have.

Anders Andersson, Dept. of Computer Systems, Uppsala University
Box 325, S-751 05 UPPSALA, Sweden +46 18 183170 andersa@DoCS.
UU.SE

✉ Re: Handwritten signatures used for verification (Hall, [RISKS-18.74](#))

Dave Finkelstein <davef@xcert.com>
Tue, 07 Jan 1997 16:51:11 -0800

I was in Las Vegas between Christmans and New Year's, and decided to purchase some sunglasses from The Sunglass Hut, a large chain of sunglass retailers in the U.S. and Canada (and perhaps other countries as well). I paid for my purchases with my Visa card, the receipt was placed in a special holder, and I was asked to sign the receipt with an electronic pen. The salesman said that they can transmit the signature during the verification process as an additional check; the signature sent is compared with what Visa has on file. I was told that the signature isn't sent always, only in circumstances where a card might be being watched for unauthorized charges.

All this information came from the salesman; I'd be interested to hear if anyone has any details about this system.

David Finkelstein, Xcert Software Inc., davef@xcert.com <http://www.xcert.com>
604.640.6210 (tel) 604.681.6220 (fax)

✶ Re: UPS use of handwritten signatures, Lauren Weinstein article

"Peter G. Neumann" <neumann@csl.sri.com>
Fri, 17 Jan 1997 9:25:52 PST

The latest issue of PRIVACY Forum Digest, Friday, 17 January 1997,
Volume 06 : Issue 02, Moderated by Lauren Weinstein
(lauren@vortex.com),
has an excellent piece of analysis on the United Parcel Service
(UPS)
use of handwritten signatures:
YOUR SIGNATURE FOR SALE? -- A PRIVACY Forum Special Report
by Lauren, who reports on the results of his investigations on
this problem.
Information on how to find that issue on the web, or to
subscribe to either
of the privacy digests is noted further on in this issue.

✶ Blaming the safety people

Joshua Levy <joshua@intrinsa.com>
Fri, 10 Jan 1997 16:35:27 +0000

Story from the Boston Globe via Institute for Global
Communications
<labornews@igc.apc.org>:

To summarize, a company's president has been arrested for

manslaughter after
two of his workers were killed in separate accidents, a year
apart. One was
pulled into a machine which lacked basic (and legally required)
safety
devices, the other was crushed by a front-end loader with
inoperable brakes.
The company had been fined hundreds of thousands of US dollars
for dozens of
previous safety violations. The RISK is contained in the
following quote.
Bowley is the president; Codinha is his lawyer:

Codinha said Bowley had ``safety officers'' working in the
junkyard when the
accidents occurred. ``This should have been their [the safety
officers']
responsibility,'' Codinha said.

This guy seems to believe that you can ignore safety laws simply
by hiring
"safety officers" and blaming them when people get killed.

Joshua Levy <joshua@intrinsa.com>

[The incidents are not particularly computer related, but the
last
paragraph may be more widely applicable than generally
realized. PGN]

⚡ The Millennium problem: another too-young case

"David R. Vinograd" <D.R.Vinograd@city.ac.uk>
Mon, 20 Jan 1997 16:56:43 +0000 (UT)

The Halifax Building Society (Savings & Loan) members who were
not sent
voting papers for conversion (to a bank) as they were too young
- born in
1890s and ages over 100 (e.g., (19)97 - (18)93 = 4). [Reported

on UK radio
last week]

David Vinograd, Director of Computing Services, City University,
Northampton
Square, London EC1V 0HB, England +44-171-477-8170 D.R.
Vinograd@city.ac.uk

🔥 Y2036, Y2038, and the superiority of UNIX

"D.J. Bernstein" <djb@koobera.math.uic.edu>
18 Jan 1997 09:00:21 -0000

In *CACM*, January 1997, page 15, Robert L. Glass reveals his shocking new discovery that UNIX time, a 32-bit signed integer representing the number of seconds after 1969 TAI, will overflow in mid-January 2038. (``And even sooner for smaller-word processors.'')

``This is one of those `surely I'm wrong' kinds of findings,''
Glass writes. ``Surely the designers of Unix anticipated such a problem and have provided for it.''

Harrumph. A certain so-called operating system stores time as a 32-bit unsigned integer representing the number of seconds after 1899. This will overflow in February 2036. Apparently Glass doesn't realize that UNIX was cleverly designed to keep on ticking for *more than a million minutes* after that other system dies of tachyon exposure.

This is all very well known to UNIX programmers. (Proof: A quick search with

DejaNews reveals that there was a ``UNIX will outlive your pathetic OS'' thread on comp.unix.advocacy, one of the most technical UNIX newsgroups, a few weeks ago. Q.E.D.)

---Dan

P.S. In all seriousness: I'm converting my data to 64-bit signed times, stored big-endian in 8 bytes, followed by 8 bytes for nanoseconds and attoseconds just in case. This won't last for more than a few hundred billion years, but neither will the Sun, and in any case I plan to throw a big programming party on 1 January 2000000001 to upgrade to 128 bits.

✉ Re: More Y2K humor: Split the difference (Brader, [RISKS-18.76](#))

Tony Lauck <tlauck@CERF.NET>
Fri, 17 Jan 1997 06:34:59 -0500

For as long as I can recall, the voter registration system in Wellesley, Massachusetts has used a three-digit field for Date of Birth. When I first saw this, I was puzzled and figured that it was probably the result of some elderly residents celebrating their 100th birthdays.

Why three digits instead of four? Were they conserving holes in punch cards?

Tony Lauck, P.O. Box 59, Warren, VT 05674
tlauck@cerfnet.com <http://www.ultranet.com/~tlauck/>

[Maybe they were hanging Chad as a warlock,

although might have better been in Salem. PGN]

✉ Re: More on fired contractor... (Horiuchi, [RISKS-18.75](#))

Carlie Coats <xcc@hpcc.epa.gov>

Fri, 17 Jan 1997 08:15:39 -0500

In many contracting situations, it is **illegal** for the contracting agency to be involved in detailed management. On EPA contracts (with which I am familiar), for example, the EPA management specifies **what** and **when** but is forbidden to even suggest **who** or **how** -- that is left for the contractor management to determine.

In such circumstances (sub-sub-contracts), the "who has been fired" information will have to traverse at least 4 layers of bureaucracy (and more probably 7-10, since in the EPA case it will go through at least 2 layers of Washington bureaucracy between the prime contractor and local project management, and maybe two more layers between local management and computer operations (and computer operations and the computer-operations contractor)).

Risk: It will take **weeks** to deal with the situation, not hours.

Carlie J. Coats, Jr., North Carolina Supercomputing Center, 3021 Cornwallis Road, Research Triangle Park, N. C. 27709-2889 1-919-248-9241
coats@ncsc.org

⚡ Re: Taco Bell-issimo ([RISKS-18.76](#))

Vincent Weaver <weave@Glue.umd.edu>

Fri, 17 Jan 1997 08:29:25 -0500 (EST)

Living in Maryland, I got the Taco Bell item on the local news. What was more interesting was what Taco Bell did upon discovering that somehow they were losing money. Apparently, instead of checking the receipts or asking the clerk, they immediately suspected it was a hardware/software problem and had technicians treat it as such. Apparently, they caught the guy only because he was bragging to co-workers about what he had done. The risks here are enormous. They actually brought a computer professor from a nearby college on the newscast to explain the risks. [And something else... the clerk had a history and a criminal record when he was hired. Taco Bell refused comment on that].

Vince Weaver weave@glue.umd.edu

⚡ IBMmail flame on -- albeit out of character

RISKS List Owner <risiko@csl.sri.com>

Mon, 20 Jan 97 7:52:22 PST

RISKS does not generally take potshots at the often miserable service provided by some of your favorite (or least favorite) Internet service providers (as well as wannabes who still don't provide decent Internet service), although we have had a few messages in RISKS on this

subject, and
on the pain that is caused -- particularly to list
administrators. This
time, my patience has run out. For a very long time, I have
been getting
bouncemail from "System Mailman" <usfmcsqc@ibmmail.com> on every
issue of
RISKS, telling me that

"Your note to SSTARKEY on FORD of [date/time] could not be
delivered
because SSTARKEY is not currently a valid userid on node FORD."

The bouncemail tells me absolutely nothing else to give me a
clue. On the
RISKS lists I maintain (at CSL) or know about (BITNET), there is
no RISKS
subscriber named STARKEY and no node named FORD. I suppose I
could bother
all of the altruistic folks who are already providing
redirection services
(.mil, .uk, .mit.edu, .xerox.com, .dec.com -- many thanks!), but
that seems
unlikely to be productive, and, besides, I should not have to do
that each
time something like this happens. [Oh, yes, you guessed
correctly; IBMmail
is not the only offender.] So, I have sent e-mail to various
addresses at
IBMmail -- including Postmaster, Action, Help, and "System
Mailman"
<usfmcsqc@ibmmail.com> -- TO NO AVAIL. So, a veil is now
withdrawn, and I
hope that by my going public, someone else will be inspired to
do something
useful -- such as one of the many IBMmail subscribers prodding an
administrator at IBMmail to modify their BARFmail facility, or
someone who
knows STARKEY telling him/her to let me know what alias is being
used, or
anything else that might help. Not only do I *not* get a
response from
IBMmail with some excuse such as perhaps that they are

incompetent or otherwise impaired, I also do not get a bounce that "System Mailman" could not receive my message. IBMmail administration seems to be a veritable electronic black hole.

IBMmail flame off. PGN

Incidentally, I'm hard-pressed to keep up with the backlog these days. (I just deleted, without reading, 15 pieces of what appeared to be unsolicited advertisements in the RISKS directory, which came in over the weekend. I just hope that none of them was a well-meaning RISKS contribution!)

I notice that AOL seems to have shot itself in the foot by going to flat-rate charges. The 17 Jan 1997 media reports indicate AOL is now asking its customers not to use their services so much, because of the difficulties of other people gaining access. Reportedly, many folks are threatening to sue because they cannot get the access they think they deserve -- and are paying for.

⚡ Re: Risks of miskeying e-mail addresses (Joseph, [RISKS-18.76](#))

Darin Johnson <darin@connectnet1.connectnet.com>

17 Jan 1997 19:15:19 GMT

When I was in grad school, I once got a letter from a professor that berated a fellow student for not attending seminars and how he'd better get his act

together if he wanted to keep working with that prof. I could not understand why I was "cc'd" on the letter, as it would have been unprofessional to do so.

Looking closer at the e-mail, I figured out what had happened. The professor had typed the subject into the "To:" field, which was something like "Please attend all ai symposiums in the future". The only thing the mail understood from that subject was that there was a mailing list called "ai", which it promptly sent the letter to (even though it was busy giving errors about the rest fo the subject).

The reply was short, "now that the whole department knows I'm lazy, can we meet in private about this?".

Why does this happen?

- Too easy to hit the final carriage return and then say oops.
- The software (generic unix mail) failed to treat the entire e-mail as faulty. If one of a group of instructions is faulty, the entire group should be invalidated.
- Mail was sent to the back-end before the addresses were verified.
- Aliases set up with the same name as common words, a longer name would have been harder to mistype.
- Apparently there was no warning that there was no subject given, or it was ignored.

The risks?

- Software systems not keeping up with society; thus a simple system for sending memos and ideas evolves into a full communications paradigm that is widely used, except it's the same old

software

with the same old assumptions.

- And of course, using easy technology for something that should have

been done the old-fashioned way. A tendency to sit behind the desk

and control the world from the console in front of you.

The old rule applies - never say anything on usenet or e-mail that you

wouldn't mind being posted in the office lunchroom. Chances are, it just

might end up there.

✉ Re: Risks of miskeying e-mail addresses (Joseph, [RISKS-18.76](#))

Niall Murphy <nmurphy@iol.ie>

Sat, 18 Jan 1997 10:14:13 GMT

The chances of mistyping an e-mail address and getting a valid one are far

higher than Gerard A. Joseph recently suggested. On Lotus CC: mail, which use

at work, as you type a name it searches for a match in a predefined list. I

am sure many other mail systems work in a similar fashion. In my case the

list includes the entire company of a few thousand users.

I have a long time friend in California, to whom I would say just about

anything. Because of distance/time difference e-mail is our main social

means of communication. His name is Michael. My boss, about whom I might

occasionally say things that I would not want him to hear (or read), also

has the name Michael. One day about five minutes after I had sent a message

to my long time friend, my boss shouted over the partition in the office -
"Hey Niall, I think you meant this mail for someone else." It took about 2 seconds to realise what had happened and 2 seconds to start sweating. I had typed Michael, and got the first Michael alphabetically. I needed only one more letter to make the name unique and then the return key made the selection. I had pressed an R instead of an M. Event though the wrong address was at the top of the message as I typed, I never noticed it.

Luckily the mail was a harmless one, but I was far more careful in future.

The risk of course is that with such a system, especially if it can be customised to select only people to whom you regularly send e-mail (I do not know enough about CC:mail to know if this can be done), then the chances become quite high that the misdirected e-mail goes to someone you know. This can easily be more embarrassing than having it go to a random person somewhere in cyberspace.

Niall Murphy

✶ Irrelevant risks of miskeying e-mail addresses (Joseph, [RISKS-18.76](#))

Lawrence H Smith <Lawrence.H.Smith@williams.edu>
Fri, 17 Jan 1997 11:22:34 -0500

While misaddressing provides trivial access to information in

the e-mail
(the unintended recipient didn't go to any effort to obtain it),
it's
irrelevant.

Far more relevant: "Nothing about the Internet" provides **any**
privacy to
any e-mail content, whether delivered to a valid address or
not. Thus, you
should **never** commit "intensely private" (or embarrassing, or
fiscal, etc.)
content to e-mail. A stamped, sealed paper mail document (or a
telephone
connection) is far more secure & reliable.

There's also no guarantee that a message sent out actually
arrives, nor that
you'll hear about it if it doesn't. It is **often** the case that
mail is
looked at only by the addressee, mail sent to a valid address
arrives there,
and you get a bounce message for invalid addresses, but there
are no
"guarantees" on **any** of this. The system works well enough most
of the time
that naive users perceive it as "like paper mail, only faster
and cheaper" -
a perception which is deeply flawed.

Lawrence H Smith, Instructional Technology Specialist, Office for
Information Technology Williams College 413-597-3073
lsmith@williams.edu

⚡ Chuq spoofing Spaf, and the archives

Adam Shostack <adam@homeport.org>
Fri, 17 Jan 1997 12:54:07 -0500 (EST)

Spaf's follow up was in 6.54, not 18.54 as noted by our
overworked moderator.

[Yes, Thanks. I fat-fingered it by force of habit -- 18 is sort of an automatic number for me in the RISKS context these days, and it was getting late. As Yogi Berra once <supposedly> said, it gets late early. I caught the error as soon as I looked at the hardcopy. It is now fixed in ftp.sri.com and catless.ncl.ac.uk archive copies, and was on the csl.sri.com website -- where only the most recent issue is available. PGN]

✦ Privacy Digests

"Peter G. Neumann" <neumann@csl.sri.com>
22 Jan 1996

Periodically I remind you of TWO useful digests related to privacy, both of which are siphoning off some of the material that would otherwise appear in RISKS, but which should be read by those of you vitally interested in privacy problems. RISKS will continue to carry general discussions in which risks to privacy are a concern.

* The PRIVACY Forum is run by Lauren Weinstein, with some support from the ACM Committee on Computers and Public Policy. He manages it as a rather selectively moderated digest, somewhat akin to RISKS; it spans the full range of both technological and non-technological privacy-related issues (with an emphasis on the former). For information regarding the PRIVACY

Forum, please send the exact line:

information privacy

as the first text in the BODY of a message to:

privacy-request@vortex.com

You will receive a response from an automated listserv system. To submit contributions, send to "privacy@vortex.com".

Information and materials relating to the PRIVACY Forum may also be obtained from the PRIVACY Forum Archive via ftp to "ftp.vortex.com", gopher at "gopher.vortex.com", and World Wide Web via: "<http://www.vortex.com>". Full keyword searching of the PRIVACY Forum Archive is available through the World Wide Web access address.

* The Computer PRIVACY Digest (CPD) (formerly the Telecom Privacy digest) is

run by Leonard P. Levine. It is gatewayed to the USENET newsgroup

comp.society.privacy. It is a relatively open (i.e., less tightly moderated)

forum, and was established to provide a forum for discussion on the

effect of technology on privacy. All too often technology is way ahead of

the law and society as it presents us with new devices and applications.

Technology can enhance and detract from privacy. Submissions should go to

comp-privacy@uwm.edu and administrative requests to comp-privacy-request@uwm.edu.

There is clearly much potential for overlap between the two digests, although contributions tend not to appear in both places. If you are very short of time and can scan only one, you might want to try the

former. If you are interested in ongoing discussions, try the latter. Otherwise, it may well be appropriate for you to read both, depending on the strength of your interests and time available.

PGN

✶ The SEI Conference on Risk Management - Preliminary Program

Carol Biesecker <cb@sei.cmu.edu>
20 Jan 1997 19:43:44 GMT

The SEI Conference on Risk Management - Preliminary Program
Managing Uncertainty in a Changing World.
7-9 April 1997
The Cavalier Hotel
Virginia Beach, Virginia

The SEI Conference on Risk Management provides a unique forum for exchanging ideas and experiences with experts and professionals who practice or study acquisition and risk management. It is a tremendous opportunity for you to increase your awareness and to advance your knowledge and skills by exposure to the latest methods, tools, techniques, and some of the best practices in the field of system development and acquisitions.

The conference is geared toward government, industry, and academic managers, practitioners, change agents, and researchers. Managers will learn how to improve their ability to make informed decisions and to gain better control of their project's cost, schedule, and technical content.

Practitioners

will increase both their awareness of risks and their ability and skills to avoid or mitigate them. Development and acquisition professionals will gain insight from the experiences of leading experts and professionals, learn about the latest developments and technological issues, and learn how to manage uncertainty in a changing world.

If you haven't attended an SEI Conference on Risk Management in the past, you may want to attend the 1997 conference. Here's why:

* Recent Congressional action as well as DoD policy emphasizes the requirement to improve acquisition practices and management of risk.

* The Fiscal Year 1996 Defense Authorization Act directs that "...the process for acquisition of information technology is a simplified, clear, and understandable process that specifically addresses the management of risk, incremental acquisitions, and the need to incorporate commercial information technology in a timely manner."

* DoD Directive 5000.1 "Defense Acquisition" (March 15, 1996) provides for "...a streamlined management structure and event-driven management process that emphasizes risk management and affordability and that explicitly links milestone decisions to demonstrated accomplishments."

For registration, contact registration@sei.cmu.edu.
For additional information about the conference, contact

SEI Customer Relations
Software Engineering Institute
Carnegie Mellon University

Pittsburgh, PA 15213

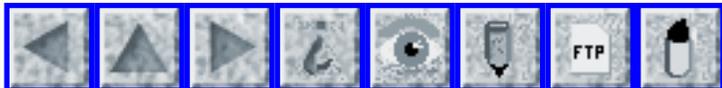
Phone, Voice Mail, and On-Demand FAX 412 / 268-5800

E-mail customer-relations@sei.cmu.edu

World Wide Web <http://www.sei.cmu.edu>

or specific questions to 412 / 268-7388

[Abridged 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 18: Issue 78

Weds 22 January 1997

Contents

- [Shetland Times copyright suit](#)
[Brian Randell](#)
- [Risks of letting NSA near your laws \(security fixes embargoed\)](#)
[John Gilmore](#)
- [A320 Flight Control Computer Anomalies](#)
[Peter Ladkin](#)
- [Lack of software testing in teaching & real world](#)
[Michael C Taylor](#)
- [Apollo date bug coming soon](#)
[Jim Rees](#)
- [Macintoshes and Y2K](#)
[Lloyd Wood](#)
- [Date overflow risks](#)
[Arthur Schor](#)
- [Y2036, Y2038, and the superiority of UNIX](#)
[Dan Hicks](#)
- [Yahoo! promotes privacy -- well, at least they make an attempt](#)
[DaVe McComb](#)
- [HTTP cookies still taste bad](#)
[Howard Goldstein](#)

- [ad.doubleclick.net -- URLs of doom](#)
[Andrew Molitor](#)
 - [Reliability of paper mail vs. E-mail](#)
[Jonathan I. Kamens](#)
 - [Caveat scriptor -- Risks of miskeying e-mail addresses](#)
[Mike Perry](#)
 - [Re: IBMmail problems](#)
[PGN](#)
[Jerry Ackels](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✂ **Shetland Times copyright suit (Re: Hoffman, [RISKS-18.64](#))**

Brian Randell <Brian.Randell@newcastle.ac.uk>

Tue, 21 Jan 1997 17:13:46 +0000

The (London) *Times* 21 Jan 1997 carries a report of the court case concerning whether the use of headlines taken from the *Shetland Times*' web site, as links back to the stories at that site, was a breach of copyright.

This article is carried in full in the electronic version of The Times, at

<http://www.the-times.co.uk/news/pages/tim/97/01/21/timlawsc101001.html?1069542>

though it may be necessary to register to get it by going in through their front door - which is at <http://www.the-times.co.uk/>

Since it is not a breach of copyright to make short extracts from an article which is in copyright, I quote:

The inclusion of the headlines of one newspaper in the internet website

of another newspaper was, prima facie, infringement of the copyright

belonging to the original newspaper.

Lord Hamilton, sitting in the Outer House of the Court of Session, so held, granting interim interdict in an action of declarator of infringement of copyright and interdict at the instance of *Shetland Times Ltd* against Dr Jonathan Wills and another.

This was under Scottish Law, and I'm not sure what an "interim interdict" is, but it sounds painful for the people who were doing the copying.

However it would seem that the judge was sympathetic to *The Shetland Times* because:

A caller gaining access to the defendants' website might, by clicking on one of those headlines appearing on the defenders' front page, gain access to the text as published and reproduced by the pursuers.

Such access was gained without the caller requiring at any stage to gain access to the pursuers' front page. Thus access to the pursuers' items could be obtained by by-passing the pursuers' front page and accordingly missing any advertising material which might appear on it.

This of course is pretty much what I'm guilty of, I guess, by giving you the direct URL of the report in the Electronic Times! :-)

What isn't clear to me from the article is whether it would be a breach of copyright to link to the articles without using the exact text of the headlines. [<http://www.ukoln.ac.uk/ariadne/issue6/copyright/> > has an earlier report.]

Brian Randell, Univ. Newcastle, Newcastle upon Tyne NE1 7RU UK
+44 191 222 7923

Brian.Randell@newcastle.ac.uk <http://www.cs.ncl.ac.uk/~brian.randell/>

✦ Risks of letting NSA near your laws (security fixes embargoed)

John Gilmore <gnu@toad.com>

Tue, 21 Jan 1997 14:15:40 -0800

Lucky Green is right in [RISKS-18.75](#). Security fixes and virus-protection software are now export-controlled. Under the old ITAR, virus-protection software was part of the list of *exempted* crypto software in XIII(b)(1)(ix). Even if it used crypto, it wasn't embargoed if the software's purpose was protection against malicious code.

In the new EAR, such software is specifically included as export-controlled under category 5D002 -- even if it doesn't include crypto!

It's now illegal to build worldwide products that are designed or modified to protect against malicious computer damage.

This sounds like a manufacturer can't even fix bugs in their products if the fix eliminates a security breach, since the fixed product is "modified to protect against malicious computer damage". This is not a joke. Everybody, it's time to call your lawyers...

It looks to me like the Information Warfare hawks have shot themselves in the foot. They were probably trying to prevent American

products from
defending foreign countries against infrastructure attacks by
the US
military. Instead, as usual, they just leave our own
infrastructure wide
open to attacks.

I encourage companies to comment to the Commerce Department
about these new
regulations. They are listening for comments by Feb 13th; see
the web
reference below for details. Don't expect your comments to
change anything;
the NSA (which is pulling the strings here) seems to *want* the
US to be
wide-open to both wiretapping and active attacks on computer-
based
infrastructure.

John

[David Holland's contribution to [RISKS-18.76](#) gave an http
address
that pointed to a draft version. John points out that the
www.epic.org URL is correct, and so is [http://jya.com/
bxa123096.txt](http://jya.com/bxa123096.txt).]

✶ A320 Flight-Control Computer Anomalies

Peter Ladkin <ladkin@TechFak.Uni-Bielefeld.DE>

Wed, 22 Jan 1997 20:05:13 +0100

The US FAA has issued a proposed airworthiness directive for
Airbus A320/321
aircraft, that the elevator/aileron computers (ELACs) be
replaced with
upgrades, to prevent uncommanded rolls during turbulence and
with specific
flap configurations. This is based on field reports forwarded to

the FAA by the Direction Generale de l'Aviation, the French FAA equivalent. Apparently, uncommanded rolls of up to 30\deg bank were experienced. It seems the upgrades are software upgrades, as might be expected.

The FAA is quoted by Aviation Week (Jan 20, 1997, p40) as saying that there are circumstances in which the sensitivity of the FBW design "creates safety concerns". Examples of such include

- * Air turbulence, with partial or full flaps set, can induce roll oscillations;
- * If full flaps are extended and subsequently jam, and partial flaps are then selected, it becomes difficult for the flight crew to maintain the selected flight path (this is surely a reference to the Dragonair incident of 6 June 1994 in Hong Kong - see Flight International, 18-24 January 1995, p40).
- * When contaminants interfere with operation of the sidestick transducer unit, transient signals from the sidestick to the ELACs may induce the ailerons to `jerk' and induce an uncommanded roll, regardless of selected autopilot mode or phase of flight.

The reference to autopilot modes is included because the ELACs are the EFCS's interface to autopilot functions. The A320 Electrical Flight Control System consists of seven major computers: two ELACs, three Spoiler and Elevator Computers (SECs) and two Flight Augmentation Computers (FACs) (info courtesy of Robert Dorsett and Peter Mellor).

This proposed Airworthiness Directive is one of only two public documents of which I am aware which details problems with the A320 EFCS. The other is the report of an incident at Sydney (Kingsford Smith) Airport in August 1991 by the (Australian) Bureau of Air Safety. In this BAS report, some user-interface anomalies with the sidestick controllers were noted. The copilot had relinquished control to the captain on an emergency go-around, had left his hand on the stick but was unaware of making any inputs. Nevertheless, the DFDR recorded copilot inputs (both neutral and nose-down pitch) for some 12 seconds. Excerpts from the report may be found in 'Computer-Related Incidents With Commercial Aircraft' <<http://www.rvs.uni-bielefeld.de>>.

I should include the usual caveats:

* Problems in control systems which are implemented by digital computers

are not necessarily problems properly to do with the computers. I would

guess that the first A320 problem above falls in this category. According

to the reports, so did the second accident to the Swedish Gripen aircraft

(see Fredriksson, [RISKS-15.26](#) and Shafer, 14.89; following Eriksson,

14.81; Thomas, 14.82; Everett, 14.85; Ladkin, 14.88; and Stalzer, 15.04),

and the X-31 accident (Ladkin, 16.89; Fuller, 17.45; Gomez, Fuller, 17.46;

Fuller, Ladkin, 17.47; Mellor, 17.60; Wright, 17.65)

* The fact that there are software upgrades does not automatically mean

that the software was in some sense 'wrong'. Such hardware is, loosely-speaking, general purpose, and one can make substantial control

system changes the 'easy' way, by reprogramming. Compare this

with the

time and expense of having to develop whole new actuators and integrate

them into the airframe, as Boeing is now doing with the B737 rudder

assembly (see `Computer-Related Incidents..'; also Aviation Week Jan 20

1997, p40; Flight International, 22-28 Jan 1997, p4).

Having said that, two of the remarked situations represent control anomalies

of a sort which may not occur with non-digital control systems.

The

Dragonair incident went unreported in RISKS. The flight-control computers

responded to pilot inputs in a different mode from that in which the

aircraft was **in fact** configured. Crudely speaking, the computers `thought'

the aircraft was flying under partial flaps, whereas in fact the flaps were

full down. In the third situation, contaminants in the pilot controls cause

jerking of the control surfaces without feedback to the pilots. This is less

clearly a circumstance which arises only with digital flight controls: for

an example with conventional control systems, consider the B737 rudder

hard-overs (incidents have been verified, and both the two unexplained B737

accidents are suspected cases). However, in a conventional control system,

contaminants **at the pilot's end of the system** would normally result in

direct feedback to the pilots. One would also expect different types of

contaminants to cause problems (no, I'm not imagining that A320 sidesticks

are susceptible to cola and coffee....). However, I suspect any case for

considering different types of contaminants to represent different failure

modes must rest on substantial differences in the type of contaminant and whence it came.

Peter Ladkin

⚡ Lack of software testing in teaching & real world

"Michael C Taylor (CSD)" <mctaylor@mailserv.mta.ca>

Wed, 22 Jan 1997 18:03:46 -0400 (AST)

One of my first 'big' projects for Mount Allison was a web interface to the Student Information System to provide access for faculty & students. During the design stage I tried to be very careful about access control and possible attacks. In December, four months after the system was in place, a student informed the HelpDesk that she wasn't receiving the correct transcript information when she requested it. She was in fact getting someone else's marks.

The source of the problem was quickly traced to the fact I had used the 'strstr' function when I should have written my own function to match the complete username. The user 'mcl' was getting the transcript of 'bmcln' instead because 'mcl' is a substring of 'bmcln'.

The second problem came when I 'fixed' it. I was not careful and provided a fix which worked only for half of the cases. Finally, another student reported having problems with getting the wrong transcript, and I fixed it in all cases.

The risks here include; using a debugged prepackaged function when it isn't appropriate. I knew the function's operation, I just didn't apply it correctly to my program, writing a program without a set of test data to search for mistakes. I only created test data to see that it 'worked', not looking for mistakes. Finally when fixing a problem, I only tested the known weakness, I did not look for other existing or new weaknesses.

I can see why the quality of software is considered so poor. Computer

Science and Programming courses do not stress testing and design specifications enough. They focus on making a program that seem to work in at least one test case. Certainly some courses do, but I completed an entire university degree including computer science without having software testing stressed in any of my courses. I am not talking formal validation, but "stress tests" used in various other engineering fields. Design specifications? Professors often gave assignments which left several points open to interpretation. Teaching by example? It is bad enough that most books and instructors do not include examples which check to see if a function failed, letting students assume 'malloc' always works.

OldRisks: Does publicizing the fact I had a system 'live' which had a serious security flaw risk future jobs opportunities because of search tools such as DejaNews? Or my poor spelling?

Michael C. Taylor <mctaylor@mta.ca> Programmer, Mount Allison University

⚡ Apollo date bug coming soon

Jim Rees <rees@umich.edu>

Tue, 21 Jan 1997 12:15:14 EST

Year 2000 is coming earlier for users of Apollo workstations. At 14:59 GMT on November 2, 1997, the high bit of the Domain/OS system clock will become set, and system bugs will prevent machines running unpatched software from booting. HP has released a fix, but it only runs on newer equipment, and has a bug of its own. Users of Apollo machines built before the dn3000 will simply be out of luck.

Details are available at <<http://pisa.citi.umich.edu/date-bug>>.

⚡ Macintoshes and Y2K

Lloyd Wood <L.Wood@surrey.ac.uk>

Tue, 21 Jan 1997 17:08:49 +0000 (GMT)

Macintosh users probably have less cause for concern about the year 2000 than any other computer users, thanks to Apple's farsighted programmers. Originally, Macs stored the date as a 32-bit number representing the number of seconds since January 1, 1904 - a scheme that wouldn't come unstuck until February 2040. But Apple's programmers decided that wasn't good enough, so modern Macs use a signed 64-bit value that can cope with any date between 30081 BC and 29940 AD - more than enough for the time being.

[Excerpted

from Newsbytes, Connected, Electronic Telegraph, 21 Jan 1997]

<URL:<http://www.sat-net.com/L.Wood/>><L.Wood@ieee.org>+44-1483-300800x3435

⚡ Date overflow risks

Arthur Schor <artschor@worldnet.att.net>

Tue, 21 Jan 1997 22:22:43 -0800

A certain set of hospital accounting packages designed in 1967 and first released in 1968 stored dates (both current and date of birth) as a signed 16-bit field representing days before or after January 1, 1900. The field overflowed in September 1989. In 1967, no one could imagine as S/360 Assembler routine being in use 22 years later. When one large service bureau had a failure because of this problem, it made *The New York Times*.

Art Schor

[Another instance of an old story in RISKS. PGN]

⚡ Y2036, Y2038, and the superiority of UNIX

Dan Hicks <danhicks@millcomm.com>

Tue, 21 Jan 1997 21:29:14 -0600

Dan Bernstein suggests keeping time in a 64-bit integer. I prefer a floating-point format -- a double-precision (64-bit) float

number that counts either the number of seconds or number of days before/after a given "epoch" date. The advantage of this format is that, while it's most accurate in the neighborhood of the "epoch", it can represent dates roughly covering the lifespan of the universe.

Dan Hicks <http://www.millcomm.com/~danhicks>

[Join the Navy if you want a floating date.
``Epochs on both your hawsers.'' PGN]

⚡ Yahoo! promotes privacy -- well, at least they make an attempt

DaVe McComb <mccomb@InterWorld.com>

Mon, 20 Jan 1997 17:50:46 -0500

When Yahoo!'s People Search page (<http://www.yahoo.com/search/people/>)

first premiered, it allowed you to look up information based on first name, last name, city, state, and phone number. Yahoo! has since removed the reverse phone number lookup, stating in their FAQ:

What happened to the "search by telephone number" feature?

We have elected to discontinue the reverse lookup feature because of privacy concerns that have been raised by users.

However, this is not actually the case -- it's still there, just in a different form.

You see, Yahoo! also allows users to suppress information about themselves,

by entering their phone number
(<http://www.yahoo.com/search/people/suppress.html>). When you enter your phone number, you get a listing containing your name and full address. By using this, you can still perform a reverse phone number lookup.

-DaVe mcombc@interworld.com Manager, Network & Security
<http://www.interworld.com/>

🔥 HTTP cookies still taste bad (Andersson, [RISKS-18.77](#))

Howard Goldstein <hgoldste@mpcs.com>
21 Jan 1997 02:46:09 GMT

Anders Andersson (Leaking WWW surfer interest profiles, [RISKS-18.77](#))

observes the possibility that the ad.doubleclick.net site, from a firm that sells space on a couple of dozen large web sites (*The New York Times* advertising column, 20 Jan 1997), may be in a position to save keyword lists submitted for search on the Alta-Vista search engine.

What Anders Andersson may not have noticed was that when the browser called up the doubleclick site it returned more than an image; it also returned a cookie that doubleclick retrieves on subsequent accesses to its affiliated systems to develop a profile of Andersson's likes, dislikes, and usage habits. [See my item in [RISKS-18.19](#) for more on these stealthy cookies.]

Seems one without too much trouble could compile an incredibly detailed profile of an individual given one's footprints through

webspaces, coupled with one's search engine habits for those inconvenient times when the footprints don't lead to doubleclick's sites. A most valuable marketing tool.

Howard Goldstein <hgoldste@bbs.mpcs.com>

[ad.doubleclick.net -- URLs of doom \(Re: Andersson, RISKS-18.77\)](#)

Andrew Molitor <amolitor@anubis.network.com>

Mon, 20 Jan 97 20:12:51 CST

I have recently noticed that many of my most commonly asked web pages (dillbert, altavista) regularly crash my graphical web browsers. Upon further investigation, I find that it is due to the advertisements inserted in these popular pages, linked to ad.doubleclick.net. (Presumably this is used by the page owner to generate some revenue.)

The trouble is that the (apparently very redundant) web server used by doubleclick occasionally serves up a GIF gratuitously, rather than respecting the HTTP protocol. This seems to crash many versions of two popular graphical browsers.

To compound the difficulty, doubleclick.net seems to have some difficulty processing mail. E-mail sent to webmaster@doubleclick.net bounced, at any rate, after several days.

The exact RISK is a little murky, but the electronic medium of the web, and its enormous popularity, seems to have made it possible for one faulty provider to seriously damage the medium.

Andrew Molitor, Network Systems

✶ Reliability of paper mail vs. E-mail (Re: Smith, [RISKS 18.77](#))

"Jonathan I. Kamens" <jik@cam.ov.com>

Tue, 21 Jan 1997 10:48:39 -0500

> There's also no guarantee that a message sent out actually arrives [...]

Neither is there any "guarantee" that a message sent on paper via the postal service will actually arrive at the correct destination or that you'll hear about it if it doesn't. We should be careful about our implicit assumptions; here, the assumption seems to be that there's more of a guarantee for paper mail ("P-mail") than for electronic mail ("E-mail").

I'm not convinced that's true.

How many times have you received P-mail that was addressed to someone else but delivered to you because the postal service screwed up or the errant mail was stuck to a piece of mail that was correctly delivered to you? I doubt there are many adults in the United States who have not experienced both of these on multiple occasions. To be sure, similar kinds of mistakes happen with E-mail, but I've never seen any concrete evidence that they

happen more or less frequently than with P-mail.

(I have, on the other hand, seen anecdotal evidence that when the postal service screws up, it often does so spectacularly. For example, I recently sent a first-class, certified, return-receipt-requested letter from Boston to New York. The postal service took 23 days to deliver the letter. When I inquired at the sending post office before delivery about the fate of my letter, they seemed surprised that I was upset about the delay, and mostly clueless about what could be done about it.

And let's not forget the articles we see occasionally in the newspaper about letter carriers dumping trailers full of mail that they didn't feel like delivering.)

One worthwhile distinction between P-mail and E-mail is that when P-mail is misdelivered, the culprit is more likely to be the postal service than the sender. With misdelivered E-mail, on the other hand, the culprit is more likely to be the sender (I'm not talking about failed delivery, which is almost always caused by some sort of system failure; I'm talking about delivery to the wrong person). What this says to me is that people are less careful about addressing E-mail than they are about addressing P-mail.

When I address a P-mail letter, I check the address, return address and postage immediately after I put them on the envelope. Then, I check them again when I pick it up from the letter holder by my door to bring it to the

mailbox. Then, I check them again before I put it in the mailbox. How many people are that careful about E-mail?

I take a somewhat callous attitude about misaddressed E-mail. "If you send E-mail to the wrong place, it's your own damn fault." Many people disagree and argue that it's the software's fault for not protecting the user from making stupid mistakes, such as the cc:Mail E-mail address completion error which was documented in another message in [RISKS 18.77](#) as well as in previous issues of RISKS.

I find that argument to be flawed. People send far more E-mail than P-mail, Any features we put in the software to make addressing errors less likely will make it take more effort to send E-mail. Users will say, "I don't want it to be so hard to send E-mail," and they'll disable the features (or become inured to them, e.g., always clicking "OK" to the "Are these addressees correct?" dialog). In fact, people have **demanded** the features which make it easier to address E-mail and which therefore make it easier to **mis*address* E-mail.

Misaddressed E-mail is going to keep happening until baby HAL grows up and we have computers that are smart enough to look at what a message says and to whom it's addressed and say, "You know, I don't think you intended to send that message where you told me to send it." In the meantime, we should all keep in mind the oft-repeated lunch-room-wall adage about E-mail.

Jonathan Kamens | OpenVision Technologies, Inc. | jik@cam.
ov.com

✶ Caveat scriptor -- Risks of miskeying e-mail addresses

<Mike_Perry@DGE.ceo.dg.com>

Wed, 22 Jan 1997 19:35:04 est

I once made a very embarrassing mistake, shortly after an internal job move, of sending a message (I thought) to my new boss, but in fact sending it to the old one, because they had the same first name, and out of habit, having typed "Alan", I went on to type the wrong surname.

I made this mistake without putting stuff in the wrong field, without any inadvertent transposition, and without, even, any assistance from partial name matching - it was all my own work.

And it got me thinking about how readily we try to slide away from the idea that we should check we've got it right before we hit the *send* key.

A smooth riding, quiet car with a powerful engine makes it easy for you to exceed the speed limit, but the judge will rightly point out that you should have been more diligent in checking the speedometer.

Mike Perry, Data General Ltd

⚡ Re: IBMmail problems

RISKS List Owner <risiko@csl.sri.com>

Tue, 21 Jan 97 9:35:56 PST

Jerry Ackels <jerrya@us.ibm.com> was very helpful in explaining the source of the IBMmail problem noted in [RISKS-18.77](#), and in ferretting out the hitherto unidentified offending address. Although **that** problem is resolved, there are many other lurking IBMmail addresses for RISKS subscribers with only a somewhat anonymous 8-character ID and no name; I suspect I will have more problems in the future. But now I know where to turn. Many thanks to Jerry, whose response follows. PGN

⚡ Re: IBMmail problems

Jerry Ackels <jerrya@us.ibm.com>

Tue, 21 Jan 1997 16:13:21 EST

Here is the problem that we are facing. When you send a note to these users and get a message back saying that the user does not exist, it looks like two valid messages to us. IBMMAIL is basically a store and forward system. It provides for ANY to ANY seamless connections between mail systems. All of the SMTP mail IDs that you listed are actually SNADS IDs. The first two letters are the ISO country code that the user is from. The rest of the characters designate enterprise and user. Our machines translate this "Inter-Enterprise Address" (IEA) into a real userid and real

node. That is,
USFMC8LM is actually SSTARKEY at FORD. You sent the SMTP note to
USFMC8LM@IBMMAIL.COM, which got to our Internet gateway and was
translated
into USFMC8LM at IBMMAIL, which got to our IBMMAIL machines and
was
translated into SSTARKEY at FORD. Then there is no way for us
to tell what
happened; this person could have left the company, changed
userid or
anything that would have deleted SSTARKEY from the AS/400 node
FORD.
MAILMAN is the userid on the FORD node that sent you back a note
letting you
know that the userid SSTARKEY did not exist. Our IBMMAIL
machines received
a note from MAILMAN at FORD, the address was changed to USFMCSQC
at IBMMAIL,
then it was sent to our Internet gateway and the address was
changed to
USFMCSQC@IBMMAIL.COM.

As you can see from this lengthy explanation, IBMMAIL sees two
messages
going back and forth. Both of them are valid messages with no
references to
any problems. In this instance, there is really nothing that we
could do.
You tried to do the right thing by sending a note to the
postmaster, you
just had the wrong address. The one that should have worked is
USFMCSQC@IBMMAIL.COM. [Apparently it did not. I tried it
several times.
PGN] This is the address for the MAILMAN ID at the system that
was
generating the error.

There is a POSTMASTER@IBMMAIL.COM userid. It is monitored.
[Yes, as I
noted in [RISKS-18.77](#), I also tried it several times. PGN] We
have searched
through the mail logs and could not find anything from your ID.
I know the

folks that monitor that ID. They do their best, but I am sure that you can imagine the kind of messages that we get. For every valid message, like yours, that we get we will get MANY that are bogus. Everything from "I am looking for my wife. I think she works for IBM, can you find her for me" to requests on how to get a job. It is these kinds of notes that make the POSTMASTER responses take so long. I assume that this happens to pretty much every service out there. We do our best to provide an excellent service, but we get thousands of these requests a week. Maybe you could put something about that in your newsletter. Let folks know that if we are spending too much time weeding through bogus messages, we don't have time to investigate and correct the valid problems. We are getting killed with vast numbers of messages, while only a VERY small amount of them are actually valid problems.

Now I will get off my soapbox and let you know what we have done. If you run into a problem where you send to an incorrect IBMMAIL address, like the one in your note, or if an address is deleted, we will send you a note letting you know what the error is and the SMTP address in question. You probably have many more IBMMAIL users than you think. We also do HOST ALIASING. Our users have the option of changing their IEA address into a more user friendly Internet-style address. They can use their own domain of a sub-domain of E-MAIL.COM. And you will never know that the message is coming from IBMMAIL unless you look through the header and

trailer info. We
will send out the same error message for these users also. [...]



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 18: Issue 79

Tues 28 January 1997

Contents

- [Spamming Risks and Solutions](#)
[Simson L. Garfinkel](#)
- [Risks of floor repair](#)
[Paul Bissex](#)
- [Computer Glitch Gives Investors Instant Loss of Balance at Schwab](#)
[Norm deCarteret](#)
- [Microsoft Office 97 Steals My Initials, MSOF](#)
[Michael S.O. Franz](#)
- [Cosmic radiation can cause computer memory loss](#)
[Martin Minow](#)
- [Re: Shetland Times copyright suit](#)
[Prabhakar Ragde](#)
[John Pelan](#)
- [Re: Macintoshes and Y2K](#)
[Bear Giles](#)
[Jonathan Stott](#)
- [Y2K on non-Unix/Microsoft systems](#)
[Steve McKinty](#)
- [Re: Y2036, Y2038, and the superiority of UNIX](#)
[Frederick G.M. Roeber](#)

- [URL filtering, Re: ad.doubleclick.net](#)
[Caveh Frank Jalali](#)
 - [Guilty by confusion? Domain names and IP addresses of net.abusers](#)
[Lars Wirzenius](#)
 - [Adios ads.doubleclick.net](#)
[John Hascall](#)
 - [Side benefit of proxies re cookies](#)
[Mark Seecof](#)
 - [Risks of communicating with the wrong person](#)
[James W. Birdsall](#)
 - [E-Mail Addressing Problems](#)
[Todd Burgess](#)
 - [Verifying Mail Addresses](#)
[David Fetrow](#)
 - [AOL software flaw](#)
[JMFBAH](#)
 - [4th ACM Conference on Computer and Communications Security](#)
[Mike Reiter](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ Spamming Risks and Solutions

"Simson L. Garfinkel" <simsong@vineyard.net>
Mon, 20 Jan 1997 20:30:41 -0800

On Monday, 13 Jan 1997, Vineyard.NET was apparently attacked by a spam-for-hire company. The organization, "CV Communications," connected to our SMTP server and started sending us advertisements for its own spamming services.

I discovered the attack after approximately 66,000 messages were sent. Most of them went to subscribers of AOL and CompuServe. I contacted the spammer, using the phone number at the bottom of each message he was

sending out, and
demanded that he stop.

Spamming is a known problem on the Internet. I'm hopeful that law-enforcement agencies will start seriously looking into this problem, as I think that there is a limit to how effective technological solutions can be.

However, there are several solutions that I have thought of.

1. Limit the number of RECV recipients permitted in each SMTP transaction.

Rather than sending out tens of thousands of messages, we were hit with a few hundred messages that each had more than 100 recipients. We have therefore modified our netperm-table file to limit the number of recipients that each SMTP connection can have.

2. Disallow transiting.

Vineyard.NET's SMTP server is used both by our customers to send out messages and by others on the Internet to send us messages. But it shouldn't be used by others on the Internet to send messages through us to third parties. We have therefore modified our SMTP server so that it can tell the difference between an internal connection and an external connection. External connections are not allowed to transit through us to other external mail servers.

3. Reject messages that come from "suspicious" sources.

We have not implemented this yet. However, it seems reasonable to reject out of hand any SMTP message from certain kinds of hosts. For

example, you might want to reject those from addresses that do not have a valid domain name, or from hosts that appear to be dialup addresses.

I have written an article about this spamming incident which will appear in my 28 Jan 1997 Packet column. You can view it at <http://www.packet.com/garfinkel> on Wednesday January 29th.

I have also made my modified SMTP server available. It is located at <http://simson.vineyard.net/hw/spam2/smap.c> . This is a modified version of the Trusted Information System's SMAP server, part of their firewall toolkit. It is my understanding that FWTK is no longer being maintained by TIS, which is a pity.

Simson L. Garfinkel, Visiting Scholar, University of Washington, Columnist for PACKET <<http://www.packet.com/garfinkel>> and The Boston Globe.

⚡ Risks of floor repair

Paul Bissex <pb@well.com>

Sat, 25 Jan 1997 13:14:16 -0800 (PST)

Last summer, contractors at Commonwealth Edison's LaSalle nuclear

power station were filling cracks in a concrete floor by pumping them

full of foam grout. What the workers didn't know, though, was that a

tunnel ran beneath that floor, carrying water for some safety systems at

the plant, and their grout was pouring through the cracks into the water.

The grout partially clogged the tunnel, compromising safety at the plant

for 10 days before Edison -- when pushed by federal inspectors -- finally

figured out what was wrong. [*Chicago Tribune**, 25 Jan 1997, front page]

The NRC levied a \$650,000 fine for what they called a "very significant

safety problem." Without getting into a debate about nuclear power, I think

one could point out the risk in thinking that there are any non-critical

jobs where critical systems are concerned.

Paul Bissex pb@well.com <http://www.well.com/user/pb/tech/>

[Grout, Grout, Dammed Slot! PGN]

✶ 'Computer Glitch Gives Investors Instant Loss of Balance at Schwab'

"Norm deCarteret (813-878-3798 (TL 438)" <nsdec@VNET.IBM.COM>

Thu, 23 Jan 97 08:06:05 EST

A program error caused Schwab's computers to omit a significant number of mutual funds when investors used Telebroker to track holdings by phone,

leading some of them to believe themselves broke. The problem existed from

Monday afternoon through late Tuesday evening scaring scores of investors.

Janus, Putnam and Schwab's own funds were among those omitted from net asset calculations.

Tracey Gordon, Schwab spokeswoman: "We were making some system changes when

there was a program error." On why the problem went on so long:
'Mutual
funds are priced once a day. We found that it would be cleaner
and simpler
to wait until the next regularly scheduled market change to
update the
system'. Cleaner and simpler for Schwab, presumably. Gordon
said investors
who made panicky trades as a result 'would be made whole' but
there'd be
risks in determining both the who and the how much.

Norm deCarteret

🔥 Microsoft Office 97 Steals My Initials, MSOF

Michael Franz <franz@UCI.EDU>
Wed, 22 Jan 1997 15:56:04 -0800

My full name is Michael Steffen Oliver Franz, which makes my
initials
"msof". I usually use these initials in internal correspondence,
and I
have an e-mail address "msof@sprynet.com".

Now, I just installed Microsoft Office 97 on my computer.

Curiously, Office 97 automatically replaces some occurrences of
"msof" by
"Microsoft Office". For example, this happens in the "initials"
box in the
Word Annotations dialog. I am not yet sure how far-reaching this
automatism
is, but the prospect of having my name replaced without my
knowledge is
frightening. You can see this strange effect for yourself if you
type "msof"
at the start of a line in Word and then wait for a short time.

Michael Steffen Oliver Franz

franz@uci.edu (university business) and msosf@sprynet.com
(private)

✂ Cosmic radiation can cause computer memory loss

Martin Minow <minow@apple.com>

Fri, 24 Jan 1997 10:08:38 -0800

An article in the Swedish newspaper Svenska Dagbladet (1997 Jan 24)

currently available on their web site <http://www.svd.se/>

describes research

carried out by Ericsson Saab Avionics by Karin Johansson that suggests that

computers, especially those carried on high-altitude aircraft flights, may

be at risk for cosmic radiation.

Johansson and her colleagues carried out experiments on SAS transcontinental

(Atlantic) flights that measured one [bit] error per memory chip per 200

hours. The article notes that a modern personal computer may have 64 such

chips. This means that an ordinary laptop PC may expect an error every three

hours, or about twice during an atlantic flight. [Assuming you brought

enough batteries.] The problem is worsened when the flight path is over the

North Pole because the earth's magnetic field, which normally protects

against cosmic radiation, is directed such that the protection is lessened.

Karin Johansson notes that the computers used to control the aircraft itself

"are not the absolutely most modern, and consequently their electronic

circuits are not as small and sensitive." However, component manufacturers are not interested in building electronics for such a small market as avionics, so the aircraft manufacturers must use the electronics available in the marketplace. To protect against error, aircraft computer designers will use parity and error-correcting circuitry to prevent a single-bit error from propagating into other computation.

Summerized and translated by Martin Minow, minow@apple.com

✉ **Re: Shetland Times copyright suit (Randell, [RISKS-18.78](#))**

Prabhakar Ragde <plragde@plg.uwaterloo.ca>

Fri, 24 Jan 1997 09:51:35 -0500 (EST)

The Shetland Times has obtained a preliminary injunction against the Shetland News to prevent the News's web site from linking to Times documents. Part of the judge's reasoning was that the advertising material on the "front page" of the Times could thus be bypassed.

I did an AltaVista search on the phrase "Shetland Times" and came up with lots of links into the depths of the Shetland Times site. Presumably DEC has committed the same offense as the Shetland News, and their new European mirror site might be vulnerable to a similar challenge.

Given the usual response to any attempts to remove "offensive" or "illegal" material from the Net, I'm surprised that I didn't turn up dozens of

third-party links into the Shetland Times site, in defiance of the reasoning behind the injunction.

Prabhakar Ragde, Department of Computer Science, University of Waterloo
Waterloo, Ontario CANADA N2L 3G1 (519)888-4567,x4660
plragde@plg.uwaterloo.ca

[There were several longer messages with similar points. PGN]

✉ Re: Shetland Times copyright suit (Randell, [RISKS-18.78](#))

John Pelan <johnp@am.qub.ac.uk>
Thu, 23 Jan 1997 20:18:45 +0000 (GMT)

The judgement, as I believe it should be interpreted, means that it is the duplication of the headlines themselves which breached the copyright law. Whether they link to the original Shetland Times articles or different articles on the same story is irrelevant. The judge believes that the headlines constitute a separate work.

It think that his decision was in line with the intention and spirit of the copyright law.

Also, I note that RISKS contributions with URLs seem to be increasingly giving away the registered account information, namely

<http://www.the-times.co.uk/news/pages/tim/97/01/21/timlawsc101001.html?10695>

This contains '10695' at the end, which is what identifies the user and

now permits anyone to access The Times site in that guise. Watch out for a change in personal preferences !

John Pelan (J.Pelan@qub.ac.uk)

[Note, in the above the '10695' is in fact a truncation of the full set of digits that were in the URL that Brian had posted. In a side message, Brian recommends that in the future that he/we indicate when such alterations are made. PGN]

✉ Re: Macintoshes and Y2K (Wood, [RISKS-18.78](#))

Bear Giles <bear@indra.com>

Thu, 23 Jan 1997 19:20:43 -0700 (MST)

>Macintosh users probably have less cause for concern about the year 2000
>than any other computer users, thanks to Apple's farsighted programmers.

This gem illustrates just how nasty the Y2K issue is. The internal representation of the date is only one small Y2K problem. The others include:

- are the library functions robust? Are they correct? (E.g., can they tell you whether 2000 is a leap year? The date of Memorial Day in 2017? The date of Easter in 2004? The number of business days between any two arbitrary dates?)
- do the developers actually call these functions, or do they write their own?
- do the developers always display 4-digit years? If not, do

they

always truncate the year correctly?

- do the developers always require 4-digit years? If not, how do they interpret shorter years?

Bottom line: if mac programs are intrinsically Y2K safe due

solely to the

representation selected by the godlike system designers at

Apple, then all

C++ programs are intrinsically bug free and fault tolerant since that

language was designed to include resources to help make software engineering

manageable.

Bear Giles bear@indra.com

⚡ Re: Macintoshes and Y2K (Wood, [RISKS-18.78](#))

Jonathan Stott <RFC822@poly.phys.cwru.edu>

23 Jan 1997 17:58:56 GMT

Ahh, but how do your applications store dates? If only the last two

digits are stored on disk then you have a problem, no matter how many bits

your system clock uses. Good hardware design only provides a false sense of

security when the programmers get sloppy.

Jonathan Stott, CWRU Dept. of Physics, School of Graduate Studies

jjs17@po.cwru.edu jstott@poly.cwru.edu <http://poly.phys.cwru.edu/~jstott/>

[~jstott/](http://poly.phys.cwru.edu/~jstott/)

⚡ Y2K on non-Unix/Microsoft systems (Wood, [RISKS-18.78](#))

Steve McKinty Sun Microsystems Grenoble <smckinty@sunicnc.France.Sun.COM>

Thu, 23 Jan 1997 15:05:49 +0100

This isn't particularly novel. DEC's VMS operating system (designed in the mid-1970s) also implements the date as a 64-bit signed integer giving the number of microseconds since the Smithsonian base date of (I think) 17th November 1858. +ve numbers are regarded as absolute values, -ve ones as deltas, but even so the VMS clock is good for many millenia.

In addition to that all date displays use a 4-digit year. There is a well-known bug filed against VMS pointing out that the date displays will be incorrect after Dec 31st 9999. The bug was accepted by DEC with the note "we will fix this in a future major architecture."

Steve

✶ Re: Y2036, Y2038, and the superiority of UNIX ([RISKS-18.78](#))

"Frederick G.M. Roeber" <roeber@netscape.com>

Fri, 24 Jan 1997 01:57:37 -0800

In [RISKS 18.78](#), Dan Hicks wrote:

> I prefer a floating-point format ...

Note that if you are measuring intervals by subtracting timestamps, then the use of floating point numbers for the timestamps can lead to hard-to-debug errors in accuracy.

The Patriot missile failure in Dhahran was caused by a similar

error: values
from the system clock (integer number of tenths of seconds since
powerup)
were converted into floating point values to do the intercept
math. After
some number of days of operation, the point floated, and the
accuracy
suffered. [See [RISKS-13.35](#)]

While it can be argued that this merely means that intervals
should not
be measured by subtraction like this, I think that floating-
point system
clocks would only increase the RISK of such an error.

Frederick G.M. Roeber, Netscape Communications Corp., 501 E.
Middlefield Rd.
Mountain View, CA, USA-94043 +1 (415) 937 3180 roeber@netscape.
com

✶ URL filtering, Re: ad.doubleclick.net ([RISKS-18.78](#))

Caveh Frank Jalali <caveh@Eng.Sun.COM>
Thu, 23 Jan 1997 14:15:38 -0800

The obvious defense against hostile or undesirable web sites is
to not visit
them in the first place. This process can in fact be automated
in
netscape's browser. This saves bandwidth and your time!

The basic premise is that the browser may optionally execute a
function on
every URL before it is accessed to determine whether a direct
connection
should be made or a proxy should be used in the process. This
affords the
opportunity to [mis]direct the browser to fetch the document
from an invalid

source. this is a good approximation of not getting the document at all.

We sit behind a fire wall, so all WWW access has to funnel through a proxy. If I tell netscape to fetch an external document using a direct connection, the connection attempt will fail, and the document will not be accessed. Netscape will put a broken image icon in its place.

Here are the nuts and bolts to do it, but some assembly is required:

Under options/network preferences/proxies, select "automatic proxy config" and tell it which file to use. Call it something like "file:///HOMEDIR/.netscape/proxy.pac", replacing HOMEDIR with your home directory; the actual code is included below. Next, go to options/general preferences/helpers and create an application helper of type "application/x-ns-proxy-autoconfig" for suffix "pac", handled by "navigator". Install this java-script code to do the actual filtering. call it "file:///HOMEDIR/.netscape/proxy.pac", as mentioned before.

=====

```
function FindProxyForURL(url, host) {
    if ( isResolvable(host) && ! shExpMatch(host, "[0-9]*" )
        return "DIRECT" ;
    else if (host == "advertising.quote.com")
        return "DIRECT" ;
    else if (host == "ad.doubleclick.net")
        return "DIRECT" ;
    else if (shExpMatch(url, "*/*/ads/*"))
        return "DIRECT" ;
    else
        return "PROXY webcache:8080; ";
}
```

✂ Guilty by confusion? Domain names and IP addresses of net. abusers

Lars Wirzenius <liw@iki.fi>

Thu, 23 Jan 1997 12:08:32 +0200

Net.abuse (spamming, mailbombing, systematic trolling, etc) are being fought via filters, among other things. This leads to unexpected risks for innocent bystanders.

Having a similar domain name as a known net.abuser can make you guilty by confusion: if a spammer operates from earthFOO.com, and you are earthBAR.com, people are going to confuse the two domains. This has already happened (for suitable values of FOO and BAR -- the common earth prefix was actually used).

If it happens in a discussion, it can be (and has been) corrected. If it happens in a router, filter, or other software, it can be difficult to even detect.

A similar thing applies to IP numbers. Many sites now block all IP addresses belonging to problematic sites. If at a later date those addresses are reclaimed by the ISP and re-assigned to another client, that client will still be blocked. Given the worries about IPv4 numbers running out, especially for smaller ISPs, this isn't unthinkable.

I have an aggressive junkmail filter (<http://www.iki.fi/liw/mail-to-lasu.html>)

You don't have to worry about it, since I've sent you mail.

⚡ Adios ads.doubleclick.net

<<john@iastate.edu> John Hascall<

Fri, 24 Jan 1997 11:29:38 -0600

I put the following in my /etc/hosts (yea, unix-centric, too bad):

```
127.0.0.1 localhost ad.doubleclick.net
```

End of problem. I suppose if not already running a WWW server one could even put in a simple script invoked by inetd :

```
#!/bin/sh
echo "Content-type: image/gif"
echo ""
cat /usr/local/etc/nyah-nyah-nyah.gif
```

if it makes you happier....

I suppose the risk is if ad-avoidance becomes popular enough that browser makers make it easy, then everyone does it, then an unintended consequence might be the hastening of the "pay-per-viewing" of the internet.

John

⚡ Side benefit of proxies re cookies

Mark Seecof <Mark.Seecof@latimes.com>

Fri, 24 Jan 1997 18:03:30 -0800

A side benefit of proxy-server/firewalls is that they somewhat mask the identity of web-browsing folks behind them. When I refuse cookies and access Internet resources through the firewall of a large

organization I get
much of the anonymity I might want. I suggest that ISP's should
offer to
proxy their small customers' browsing just to give them this
benefit.

✂ Risks of communicating with the wrong person

"James W. Birdsall" <jwbirdsa@picarefy.picarefy.com>

Thu, 23 Jan 1997 20:19:11 -0800

Actually, the risks of misaddressing occur in any communication
medium. We
all receive paper mail that isn't for us; since most of us check
addresses
before opening mail, privacy is usually preserved at least (as
it would be
if we used the electronic equivalent of envelopes --
encryption). We all
receive phone calls that aren't for us; since the telephone is an
interactive medium it is customary to verify the identify of the
person at
the other end before exchanging messages, thus preserving
privacy and
ensuring that the message reaches the right person.

In 18.77, darin@connectnet1.connectnet.com (Darin Johnson)
writes:

>The old rule applies - never say anything on usenet or e-mail
that you
>wouldn't mind being posted in the office lunchroom. Chances
are, it just
>might end up there.

Actually, the place where this event is most common is on the
MU* (MUD,
MUSH, MUCK, MOO, MUX, etc.) systems, where it is known as a
"mav". When
sending a private message (page, whisper) to someone, it is very
easy to 1)

send a message to the wrong person, typically somebody else you are talking to or 2) mistype the command so everybody in the room sees the message. On fancier systems which allow a user to automatically reply to the last person who paged them, it is common (especially when the net is lagging) to get a page from person B while typing a reply to person A and thereby accidentally send the reply to person B.

Despite a lot of fallout and embarrassment from these incidents, nobody has come up with a good way of reducing them -- if people won't double-check what they type, there's nothing software can do to save them.

Also in 18.77, Lawrence.H.Smith@williams.edu (Lawrence H Smith) writes:

```
> ... naive users perceive it as "like paper mail, only faster  
and cheaper" -  
> a perception which is deeply flawed.
```

Actually, the perception that paper mail is reliable is deeply flawed.

Comparing the performance of the US Postal Service to that of the net in my nine-plus years on the net, I would have to say that paper mail is at least as bad if not worse. The post office loses several pieces of mail on me every year. Their latest goof-up was to misdeliver a piece of mail to the wrong address (wrong *state*, even!) three times before bouncing it back to me. Now, this failure mode is shared by electronic mail, but the post office took two months as opposed to a few hours.

--James W. Birdsall

⚡ E-Mail Addressing Problems

Todd Burgess <tburgess@uoguelph.ca>

Thu, 23 Jan 1997 23:07:10 -0500 (EST)

The university of Guelph has a simple policy for creating e-mail accounts:

first initial, last name (i.e., tburgess@uoguelph.ca). This scheme works

great as long as there are no duplicates (ie Tom Burgess). If there are

duplicates then they start adding numbers to the e-mail ID or simply using

first names.

When my brother came to Guelph my Dad tried sending e-mail to jburgess@uoguelph.ca which was not my brother's e-mail account. My brother

had been given the account joel@uoguelph.ca. Luckily the person who got the

e-mail was nice enough to look up the correct address and forward it to my

brother.

The RISKS? E-mail ID schemes like this work great as long as there are no

duplicate names. The moment there are duplicate names then a lot of people are

going to start seeing other people's e-mail.

As for Kamens's ([RISKS 18.78](#)) comment about paper mail vs. e-mail. I think

it would be fair to say that it is easier to get an e-mail address wrong

than a paper address wrong. E-mail delivery systems only have the e-mail

address to go on when delivering mail. If your e-mail ID doesn't match then

tough it bounces.

Mail addresses have fields like name, address, city, country and

postal code
to assist in delivering mail. Failing that post offices can open
mail in
hopes of finding the correct address. I know people who have
worked in post
offices in small towns and they say they can usually determine
where to send
a letter simply on the name alone (even if the address is
incorrect or
missing).

University of Guelph, Computer Science Major E-mail:
tburgess@uoguelph.ca
URL: <http://eddie.cis.uoguelph.ca/~tburgess>

✈ Verifying Mail Addresses

David Fetrow <fetrow@biostat.washington.edu>
Fri, 24 Jan 1997 21:26:55 -0800 (PST)

In [RISKS-18.78](#) Mike_Perry@DGE.ceo.dg.com and others discuss the
problem of
verifying e-mail addresses as correct, rather than just hitting
the send key.

The obvious solution ("Do you really want to send this? y/n")
would
undoubtedly work no better than it does for file deletion.

It occurred to me that perhaps what's needed is verifying
something besides
words on the screen; that if I am dealing with two kinds of
sensory data
something is more likely to click. e.g. a voice saying:

"Sending mail to Ann Landers <al@annland.org>, OK?" and my
saying "yes" or
"no" (well within a modern machines abilities). Perhaps even do
a little

scan for hot words and have it ask: "Do you really want to use the word 'braindead' in your mail to 'boss'?".

Although this is probably silly regarding e-mail (and adds a host of risks of its own) such warnings attached to particularly risky commands and forcing a person to do something *unusual* to continue could prevent a lot of errors, if not overused.

(Note, something similar happens when the WinNT 4.0 license appears on the screen while installing that product. To continue you have to hit F8, and only F8. You are pretty much forced to at least glance at the license in order to continue. Annoying but rather slick. Taking it one step further: the key needed could be chosen at random from the non-letters.)

David Fetrow, Biostatistics, University of Washington

✂ AOL software flaw (Re: PGN comment in [RISKS-18.77](#))

JMFBAH <jmfbah@aol.com>

Thu, 23 Jan 1997 09:30:15 -0500 (EST)

> ... AOL seems to have shot itself in the foot by going to flat-rate charges.

Complicating the access problem (which I haven't experienced personally) is that AOL keeps putting up a piece of software that seems to block internet traffic. Despite repeated attempts to explain the problem, this software

still appears (almost every other day) without the original problems getting fixed. I believe it's very hard to determine whether the new pricing has anything to do with their problems as long as they keep putting up software that doesn't work.

/BAH

⚡ 4th ACM Conference on Computer and Communications Security

Mike Reiter <reiter@research.att.com>

Thu, 23 Jan 1997 22:03:33 -0500 (EST)

*** EARLY REGISTRATION DISCOUNT ENDS JANUARY 31 ***
Fourth ACM Conference on Computer and Communications Security
(Preliminary Technical Program)
Zurich, Switzerland
April 1-4, 1997
Sponsored by ACM SIGSAC

For more information, including registration and hotel information,
see: <http://www.zurich.ibm.ch/pub/Other/ACMsec/index.html>

[The program looks really interesting. PGN says, "check it out."]



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 18: Issue 80

Saturday 1 February 1997

Contents

- [Berkeley student Ian Goldberg takes 3.5 hours to crack RC5 40-bit key](#)
[press release](#)
[via John van Heteren and Al Stangenberg](#)
- [Non-Anglo Names Confound U.S. Social Security](#)
[Scott Lucero](#)
- [Spelling checkers and inconsistent interfaces](#)
[Geoff Kuenning](#)
- [Electronic Funds Transfer without stealing PIN/TAN](#)
[Debora Weber-Wulff](#)
- [Corel warns about Word macro viruses](#)
[Yves Bellefeuille](#)
- [RISKs of virtual patients](#)
[Nick BROWN](#)
- [CSR hit by Year 2000 bug](#)
[Norman Fenton](#)
- [Malicious Net Software Leads to Big Telephone Bills](#)
[Jeff Uphoff](#)
- [Re: New US regs ban downloadable data-security software](#)
[Ian Goldberg](#)
- [The Risk of Changing a Mailing List](#)

[Chris Meadows](#)

● [MS Office steals my initials - Follow-up](#)

[Michael Franz](#)

● [MCI as ISP, some security concerns...](#)

[Helen Stewart](#)

● ["Moths to the Flame" by Rawlins](#)

[Rob Slade](#)

● [Info on RISKS \(comp.risks\)](#)

⚡ **Berkeley Student Ian Goldberg Takes 3.5 Hours to Crack RC5 40-bit Key**

Al Stangenberger <forags@nature.berkeley.edu>

Fri, 31 Jan 1997 10:49:25 -0800 (PST)

[John van Heteren vanhet@sirius.com found this press release on

<http://www.urel.berkeley.edu/releases/> and sent it to comp.dcom.telecom .]

Berkeley -- It took UC Berkeley graduate student Ian Goldberg only three and a half hours to crack the most secure level of encryption that the federal government allows U.S. companies to export.

[On 28 Jan 1997] RSA Data Security Inc. challenged the world to decipher a message encrypted with its RC5 symmetric stream cipher, using a 40-bit key, the longest keysize allowed for export. RSA offered a \$1,000 reward, designed to stimulate research and practical experience with the security of today's codes.

Goldberg succeeded a mere 3.5 hours after the contest began, which provides very strong evidence that 40-bit ciphers are totally unsuitable

for practical security. "This is the final proof of what we've known for years: 40-bit encryption technology is obsolete," Goldberg said.

RSA's RC5 cipher can however be used with longer key sizes, ranging from 40 to 2,048 bits, to provide increasing levels of security.

U.S. export restrictions have limited the deployment of technology that could greatly strengthen security on the Internet, often affecting both foreign and domestic users, Goldberg said. "We know how to build strong encryption; the government just won't let us deploy it. We need strong encryption to uphold privacy, maintain security, and support commerce on the Internet -- these export restrictions on cryptography must be lifted," he said.

Fittingly, when Goldberg finally unscrambled the challenge message, it read:

"This is why you should use a longer key."

The number of bits in a cipher is an indication of the maximum level of security the cipher can provide, Goldberg said. Each additional bit doubles the potential security level of the cipher. A recent panel of experts recommended using 90-bit ciphers, and 128-bit ciphers are commonly used throughout the world, but U.S. government regulations restrict exportable U.S. products to a mere 40 bits.

Goldberg used UC Berkeley's Network of Workstations (NOW) to harness the computational resources of about 250 idle machines. This allowed him to test

100 billion possible "keys" per hour -- analogous to safecracking by trying every possible combination at high speed. This amount of computing power is available with little overhead cost to students and employees at many large educational institutions and corporations.

Goldberg is a founding member of the ISAAC computer security research group at UC Berkeley, which is led by assistant professor of computer science Eric Brewer. In the fall of 1995 the ISAAC group made headlines by revealing a major security flaw in Netscape's web browser.

[This item appeared more or less intact in various news media. Ian also

was featured in a live hookup at the RSA Data Security Conference on 29 Jan,

and noted that the key was found after exhausting only 30% of the keyspace.

2**41.5 workstation-microseconds were expended, at a rate of 1 million

keys every 6 seconds. Nifty piece of work. Incidentally, longer RC5 key

lengths have increasingly higher prizes, and may still be up for grabs.

Also, as I recall, one DES key is worth \$10,000. PGN]

[Typo in title fixed in archive copy. PGN]

⚡ Non-Anglo Names Confound U.S. Social Security

lucero <lucero@optec.army.mil>

Wed, 29 Jan 97 11:20:25 EST

An internal Social Security Administration (SSA) report described in the 17

Jan 1997 *Washington Post* states that \$234 billion worth of wage reports, some going back to 1937, cannot be matched to individual accounts. The wage reports are used to compute benefits. The San Bernadino SSA District Headquarters states that their computer system is 'confounded' by Asian, Latino, Native American and Islamic names. Surnames with spaces, such as 'de la Rosa' or where the surname is not at the end of the name, such as 'Park Chong Kyu' are typical of those mishandled. Women who change their names when getting married also constitute a large portion of the errors. The San Bernadino office has corrected 100,000 mismatches of the 200 million unmatched wage reports.

Rep. George E. Brown Jr. has sought a General Accounting Office investigation, but has been blocked by House Ways and Means Committee Chairman Bill Archer.

The RISK here is designing a system for a diverse population without considering procedures to handle that diversity.

Scott Lucero, U.S. Army Operational Test and Evaluation Command

⚡ Spelling checkers and inconsistent interfaces

Geoff Kuenning <geoff@Ficus.CS.UCLA.EDU>
Fri, 31 Jan 1997 12:51:38 -0800

A posting on the Orchestra List once again highlights the RISKS of inconsistent interfaces:

> From: Symph@uwyo.edu (Michael T. Griffith)
> To: orchestralist@hubcap.clemson.edu (ork)
> Subject: spellcheckers
...
> I know some of you have been amused (at best) by my
spellchecker episodes
> in the past few weeks (Hindemith came out as Hindmost was the
worst). If
> you're interested, I've discovered the problem, and will share
it with
> Microsoft Mail users out there.
>
> In MS Word, if the spellchecker highlights a word it doesn't
know, like
> Hindemith, you can click on "add" and it puts Hindemith into
its dictionary
...
> In MS Mail, if it highlights a word it doesn't know, and you
click on "add,"
> it puts the highlighted correction it offered into the
dictionary as a
> permanent correction. Since "Hindmost" was the first offered
correction, it
> permanently noted that every time I type Hindemith, it would
substitute
> Hindmost.

So in one interface, "add" means "add this word, as-is, to the
dictionary."

In the other, "add" means "add this suggested replacement to the
dictionary
and never ask me again."

Incidentally, ispell users have been asking for the latter
feature for
years, but I have stubbornly refused because I think that
automated
replacement is far too RISKY to trust a computer.

Geoff Kuenning g.kuenning@ieee.org geoff@ITcorp.com
<http://fmg-www.cs.ucla.edu/geoff/>

[Hindemith wrote "Mathis der Maler". Hindmost wrote "MS der

Mauler",
seemingly applicable in English (one who mauls). Although not quite
echt deutsch, there are several potentially pertinent interpretations
as well. PGN]

✶ Electronic Funds Transfer without stealing PIN/TAN

Debora Weber-Wulff <weberwu@tfh-berlin.de>

1 Feb 1997 05:12:02 GMT

The Berlin newspaper "Tagespiegel" reports on 29 Jan 97 about a television
show broadcast the previous evening on which hackers from the Chaos Computer
Club demonstrated how to electronically transfer funds without needing a PIN
(Personal Identification Number) or TAN (Transaction Number).

Apparently it suffices for the victim to visit a site which downloads an
ActiveX application, which automatically starts and checks to see if
Quicken, a popular financial software package that also offers electronic
funds transfer, is on the machine. If so, Quicken is given a transfer order
which is saved by Quicken in its pile of pending transfer orders. The next
time the victim sends off the pending transfer orders to the bank (and
enters in a valid PIN and TAN for that!) all the orders (= 1 transaction)
are executed -> money is transferred without the victim noticing!

The newspaper quotes various officials at Microsoft et al expressing
disbelief/outrage/"we're working on it". We discussed this briefly in class

looking for a way to avoid the problem. Demanding a TAN for each transfer is not a solution, for one, the banks only send you 50 at a time, and many small companies pay their bills in bunches. Having to enter a TAN for each transaction would be quite time-consuming. Our only solution would be to forbid browsers from executing any ActiveX component without express authorization, but that rather circumvents part of what ActiveX is intended for.

A small consolation: the transfer is trackable, that is, it can be determined at the bank to which account the money went. Some banks even include this information on the statement, but who checks every entry on their statements...

Debora Weber-Wulff, Technische Fachhochschule Berlin,
Luxemburger Str. 10,
13353 Berlin GERMANY weberwu@tfh-berlin.de <<http://www.tfh-berlin.de/~weberwu/>>

[Now you can get a TAN even in the dead of winter! PGN]

⚡ Corel warns about Word macro viruses

Yves Bellefeuille <an448@FreeNet.Carleton.CA>
30 Jan 1997 05:03:46 GMT

In an advertisement in the latest issue of Time magazine (3 February 1997, Canadian edition), Corel mentions the existence of Word macro viruses as a reason to prefer WordPerfect:

Virus Free* -- Steer clear of the recently identified Microsoft (r) Word macro viruses. With Corel WordPerfect Suite 7 and Corel Office Professional 7, it's safe to share documents with your co-workers.

[* Source: *_WordPerfect for Windows Magazine_*, November 1996, p. 21]

It will be interesting to see if WordPerfect really does profit from this problem. Personally, I'm still using WordPerfect 5.1 for DOS! ;-)

Yves Bellefeuille, Ottawa, Canada an448@freenet.carleton.ca
<http://www.ncf.carleton.ca/~an448/>

⚡ RISKS of virtual patients

+33)388412674 <"Nick BROWN" <Nick.BROWN@DCT.coe.fr> (Tel>
27 Jan 1997 15:17:43 +0000

According to BBC Radio 4's "Today" programme this morning (January 27th 1997), a hospital in Bristol, England, has created a "medical simulation centre". The flagship effort of this centre is a "patient simulator" on which medical students, doctors, nurses, paramedics, etc can "practise"; the idea being, presumably, to make the really bad mistakes before getting to real live patients, similarly to how airline pilots are trained.

The following points came to mind as I listened to the centre's spokesperson presenting this huge breakthrough in medical training:

1. To what extent will the bedside manner of many doctors be enhanced by

training on an unfeeling robot ?

2. The simulator apparently cost GBP 250,000. Does anyone else feel that US\$400,000, or two person-years of relatively inexpensive systems consultant time, is perhaps on the low side for a full simulation of what took evolution several million years to achieve ? Or maybe the simulation is perfect and only the centre's accounting software has problems ?

3. Anyone want to be next month's paycheck that administering 32767 milligrams of any substance to the simulator will not cause a previously present, non-zero quantity of that substance to go negative and thus disappear ? Once medical students discover that a blood alcohol level of 200 milligrams can be reduced by administering the equivalent of six bottles of vodka, how many will go out and try it, and then sue the simulator's programmers ?

Nick Brown, Strasbourg, France

✶ CSR hit by Year 2000 bug

Norman Fenton <nf@csr.city.ac.uk>
Tue, 28 Jan 1997 23:19:07 +0000

[Forwarded with permission by Pete Mellor <pm@csr.city.ac.uk>.]

Can you believe that we have already been hit by a Year 2000 bug? Today I went with my part-time PhD student to the library and her card was rejected. This is because her card expiry date is the year 2000

which,
according to the library computer entry system, is 1900, i.e.,
her card is
rejected for being out of date. (She actually has got a print-
out which
states that her card expires in 1900.)

Apparently the problem is known to library and security* staff
but they have
not done anything about it. Considering how new** the library
is, is it not
incredible that such a serious and obvious year 2000 bug was not
avoided?

Norman

[Explanatory annotations from Pete Mellor:]

* Our identity cards, which should be worn at all times within
the
university, are dual purpose, and serve as library cards also.
The library
identifies the owner by a bar-code. There is a magnetic strip on
the back,
which is not (at the moment, as far as I am aware) used for
anything. For
staff on fixed term contracts, an expiry date is shown on the
card and held
on the database.

** The library has just undergone major refurbishment and
extension, and
installed a new computer system.

Peter Mellor, Centre for Software Reliability, City University,
Northampton
Square, London EC1V 0HB, UK. +44 (171) 477-8422, p.mellor@csr.
city.ac.uk

⚡ Malicious net software leads to big telephone bills

Jeff Uphoff <juphoff@tarsier.cv.nrao.edu>

Thu, 30 Jan 1997 17:39:31 -0500

http://www.thestar.com/thestar/editorial/money/970129C01c_FI-PORN29.html

Porn on Net leads to big bills;

Overseas phone flip boosts phone bills, police say

By Robert Brehl - Toronto Star Business Reporter, 29 Jan 1997

A bizarre scam involving pornography on the Internet has cost victims

hundreds of dollars, Royal Canadian Mounted Police say.

Some victims have been unknowingly charged up to \$1,200 to download

porn from the Web site (sexygirls.com), said Corporal Marc Gosselin,

of the RCMP's computer crime unit.

Gosselin said the scam worked this way:

The website informs Internet surfers that looking at nude pictures is free.

To see the pictures, ``a special image viewer'' must be clicked on and

downloaded to your home computer.

``And that's a virus, a Trojan horse,'' the Mountie said.

When it is clicked on, the viewer's modem is disconnected from the

regular local Internet service provider, Gosselin said.

Then the dialer volume is turned off, and a phone number in Moldova,

in the former Soviet Union, is dialed.

Surreptitiously, the person's computer in Canada is then hooked to a

phone number in Moldova, Gosselin said.

>From Moldova, the call is bounced back to a computer in Scarborough where the pornographic pictures are stored.

``You're accessing a server in Scarborough through a long-distance call to Moldova,'' Gosselin said.

The scam can continue even after viewing the pornography.

That's because Internet surfers may move on to other Internet sites, but are still unknowingly connected to Moldova and racking up long-distance charges, Gosselin said in an interview from Montreal.

Because the investigation is continuing and charges are pending, the Mounties refuse to name the company in Scarborough.

The Star attempted to send an E-mail to officials connected to (sexygirls.com). The page has an area for sending E-mail, but would not accept electronic messages from The Star.

The website boasts having had more than 1 million visitors since Jan. 1, 1997. That number could not be verified.

The RCMP has ordered that all calls from Canada to the number in Moldova not be connected, so this scam has been stopped, the corporal said.

But telecommunications experts say oodles of other potential scams are out there, and consumers should beware.

Ian Angus, author of the book Phone Pirates, said using the Internet is the latest twist in scamming people on long-distance charges.

``It's not just a dirty trick, it's business, big money,'' Angus

said.

That's because it's common for phone companies in foreign countries to try to attract calls from the lucrative North American market, he said.

Bell will look at each case before deciding whether to waive the charges

Typically, foreign phone companies enlist entrepreneurs to generate calls and then, in turn, pay the entrepreneurs a percentage of each call.

Canadian phone companies ``must pay international settlement charges to foreign countries even if they can't collect at home,'' said Angus, president of Angus Telemanagement.

Bell Canada spokesperson John Peck said the company will look at each complaint before deciding whether to waive the charges.

``But we're on the hook for it, too,'' Peck said. ``Chances are the individual will be held responsible.''

If Bell waived the charges, other Bell customers and shareholders would be subsidizing the charges rung up, unknowingly or not, by people downloading pornography.

Gosselin and Angus said Bell probably won't get too many complaints because of the embarrassment factor for victims forced to admit what they were doing in order to argue for a rebate.

The RCMP has had 20 complaints so far, but hundreds of others have probably been taken, Gosselin said.

He said it would be several weeks before any charges are laid related to unauthorized access to computers and fraud.

⚡ Re: New US regs ban downloadable data-security software

Ian Goldberg <iang@cs.berkeley.edu>
Mon, 13 Jan 1997 17:45:38 -0800 (PST)

Lucky Green ([RISKS-18.75](#)) said:

> The new US crypto export regulations control the export of most if not all
> data-security software. Regardless if the software uses cryptography or
> not. Many software archives seem to be in violation of the new regs. [...]
> This certainly controls virus checkers, firewalls, and other security
> software. There are substantial penalties involved in violating the EAR.
> The US can assess daily penalties and block all exports of a company's
> non-violating products. Criminal penalties apply as well.
>
> "Export", as defined in the new regs, includes making software available on
> the web or via ftp.

After very careful reading of the Export Administration Regulations (EAR) (though IANAL), it would seem that the above is slightly inaccurate.

Although, as Lucky pointed out, virus checkers et al. are indeed regulated for export from the US, and putting software up for ftp or WWW is considered

export, the EAR does not apply to "publicly available" software (732.2(b)(1)). Software is publicly available "when it is available for general distribution either for free or at a price that does not exceed the cost of reproduction and distribution" (734.7(b)).

Therefore, it would seem that, as long as the security software on your ftp or WWW site is free of cost, it is OK to keep it there. Commercial security software, however, remains export-restricted.

NOTE, however, that products that actually do contain cryptography fall under an exception (734.7(c)): "Notwithstanding paragraphs (a) and (b) of this section, note that encryption software controlled under ECCN 5D002 for ``EI'' reasons on the Commerce Control List (refer to Supplement No. 1 to part 774 of the EAR) remains subject to the EAR even when publicly available."

The software controlled for EI reasons under 5D002 are described as: "EI controls apply to encryption software transferred from the U.S. Munitions List to the Commerce Control List consistent with E.O. 13026 of November 15, 1996 (61 FR 58767) and pursuant to the Presidential Memorandum of that date. Refer to Sec. 742.15 of the EAR."

As virus checkers et al. were not on the Munitions List, they are not controlled for EI (Encryption Items) reasons, but rather for NS (National Security) and AT (Anti-Terrorism) reasons.

The RISKS: the government suddenly creating (and putting into effect) new

rules covering large amounts of software, without warning or (in my opinion) justification.

- Ian "again, IANAL"

⚡ The Risk of Changing a Mailing List

"It's a thingie! A fiendish thingie!" <c684459@cclabs.missouri.edu>

Thu, 30 Jan 1997 08:37:20 -0600

I subscribe to the Timecast Times mailing list, a fairly low-volume but large-size announcement mailing list I'm on. It's not a discussion list but an announcement list--usually, it sends one ~5-10K file through, once a week. Last night, one of these announcement posts bounced, and the bounce apparently went out to the entire Timecast Times list.

I didn't think too much of this e-mail bounce, hardly even glanced over it.

But this morning, I received about eight more message from said list, mostly from subscribers saying "Please take me off this list!", some of whom quoted the entire 8K announcement file along with their message.

Taking a closer look at the messages revealed something rather interesting.

Cause of the bounces aside, the message at the end of Timecast Times that used to state:

```
> ** To remove yourself from this mailing list, send a message to
> tctimes@prognnet.com with
>
> UNSUBSCRIBE your_e-mail_address
>
```

> on a single line in the body of the message. **

now reads

> For help subscribing, unsubscribing, and changing your e-mail
address,
> send e-mail with the word "Help" in the subject line to
> tthelp@direct.timecast.com. You will receive an automatic
response with
> instructions.

From this, it looks like they've had to change their mailing
list software
when they changed the site the list was running from.

Offhand, I'd say there are two major RISKS to be seen in this:

RISK #1 can be found in the advice that when you're switching
mailing list
software, it would be a good idea to know what you're doing.
Looks to me
like misconfiguration caused bounces to be sent through the list
to its
subscribers, instead of to the listowner alone; e-mail replies
to the list
to be sent to the subscribers rather than just the listowner;
and maybe even
the original bounces in the first place. The RISK here is that
misconfiguration can lead to mess-up.

RISK #2 advises that you should make it as easy to unsubscribe
as you
possibly can. Firstly, instructions should be at the
beginning of the
message...if you don't want to be receiving the thing, are you
really going
to read it down all the way through the end? Second, it should
be clear-cut
and self-evident what to do just by looking at it. "For help, e-
mail here"
just doesn't cut it. The RISK here resides in people's inherent
tendency
toward laziness: People don't want to work to get off a list

like this,
they're going to hit that big old 'R' key and say "Take me off,
now!"
instead, probably quoting the entire message in the hopes of
filling up the
mail spool of whoever they're replying to.

When you combine the RISK of misconfiguration with the RISK of
obfuscation,
you get a snowball effect as more and more people reply quoting
the entire
message, causing more and more mailboxes to fill up or more time
to be spent
downloading junk e-mail, causing more and more people to reply...

Chris Meadows aka Robotech_Master robotech@jurai.net
robotech@eyrie.org
<http://www.eyrie.org/~robotech/index.html>

✶ MS Office steals my initials - Follow-up

Michael Franz <franz@UCI.EDU>
Thu, 30 Jan 1997 16:06:47 -0800

Thanks to the more than 100 people who replied to my posting
(many of them
to my msof-address :-).

Many of you suggested that msof might be in my "AutoCorrect"
word list, and
some were wondering who had put it there. It turns out that the
problem is
related, but not due to "AutoCorrect". It seems that Word97 not
only has an
"AutoCorrect" feature, but also an independent "AutoText" with
"AutoComplete" feature, and this is what's causing the visible
substitution
effect. AutoText has a word list that includes such wonderful
phrases as

Best Regards,
Dear Mom and Dad,
Dear Sir or Madam,
Love,
and, yes, you guessed it,
MSOffice.

When you have AutoComplete turned on, which is the default after installation, anything you type that matches an AutoText entry is expanded when you press Enter or Tab. For example, typing the four letters "to w" (with a blank between o and w) and then the Tab key, will yield the string "To Whom It May Concern:" on your screen.

This still doesn't explain, however, why the MS Office installer performs such auto-text expansions on existing user-preference files when upgrading from Word 95 to Word 97. Might it be that, internally, this is actually performed by parsing the old configuration file and writing out a new one *using Word itself*? Then, if the new-configuration-writer would type msof followed by a Tab or a Return, you would get MSOffice...

Michael Franz franz@uci.edu

⚡ MCI as ISP, some security concerns...

Helen Stewart <helen@ptolemy-ethernet.arc.nasa.gov>

Mon, 27 Jan 97 09:02:55 PST

Yesterday, I registered my mother to MCI as an ISP. They create your access codes, which are long mixed characters, for what they call security. They aren't very informative about how to use the services or an

explanation on
your user codes, they ask for you to create a code or phrase in
the
beginning on registering, for authentication if you have
problems with
service etc. They also give you your first.lastname as your
userid.

So, I accessed the MCI server with the strange code, but when I
got to my
mothers e-mail stuff there was another code they created for
security, but
it wouldn't authenticate. So, I called them telling them I was
my mother
and asked for the username code and password code. The only
thing they
asked me for was my mother's home address prior to giving me the
codes! I
could have been anyone asking for the username codes and
passwords! They
gave me both codes, one for accessing the server and the e-mail
one!

What worries me about all this, is that it doesn't take much to
know if
someone has an account on MCI and get their address? Then, just
call in
saying that you forgot your codes and then login, purchase MCI's
products
online using the credit card that you gave MCI to bill you
monthly? Right?

The funny thing is that they earlier asked for a phrase etc. for
service...
but they didn't ask me for it? They didn't ask me for the
accounting codes
or service codes that they provided after registration on the
browser? Just
the physical home address?

Is this dangerous or what? I immediately had my mother cancel
the service
with them. Please look into this and see if they do this to

other people?

I am worried how easy it is to do this with other providers
other than MCI?

Helen Stewart

✈ "Moths to the Flame" by Rawlins

Rob Slade <roberts@mukluk.hq.decus.ca>

Mon, 27 Jan 1997 13:08:37 EST

BKMTFLM.RVW 961021

"Moths to the Flame", Gregory J. E. Rawlins, 1996, 0-262-18176-2, U\$22.50

%A Gregory J. E. Rawlins rawlins@cs.indiana.edu
%C 55 Hayward Street, Cambridge, MA 02142-1399
%D 1996
%G 0-262-18176-2
%I MIT Press
%O U\$22.50 curtin@mit.edu
%P 184
%T "Moths to the Flame"

From the subtitle, "The Seductions of Computer Technology", one can, perhaps, assume that the book is not going to be an unalloyed apologia for the computer. Poor old technology seems to be a popular stuffed lion to kick these days. Rawlins' book, more like a series of articles, is more informed and erudite than most, but readers of, say, the RISKS-FORUM Digest will find this to be thoroughly plowed ground.

Rawlins looks at encryption (rather well, actually), virtual reality, information technology, the net, weapons technology, and employment.

Chapter 7 gets a little out of hand: it finishes with two (not terribly good) science fiction "cautionary tale" set pieces. The final chapter moves out into the realm of technology in general, but returns to a bit more balanced view.

copyright Robert M. Slade, 1996 BKMTHFLM.RVW 961021
roberts@decus.ca rslade@vcn.bc.ca
rslade@vanisl.decus.ca

Please note the Peterson story - <http://www.netmind.com/~padgett/trial.htm>

[Only one bit more? Maybe he bit off more moths than he could shoo. 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 18: Issue 81

Thursday 6 February 1997

Contents

- [The \(f\)e-mail of the PCs is more deadly than the bail](#)
[PGN](#)
- [Difficulties in developing large systems: IRS, etc.](#)
[PGN](#)
- [E-mail saboteurs confuse Columbian kidnapping negotiations](#)
[Miranda Mowbray](#)
- [Dutch bank folly](#)
[Sape Mullender](#)
- [Will-o'-the-w-ISP! More on AOL, Cyber Promotions](#)
[PGN](#)
- [AOL: 45 minutes and Out -- w/glitch](#)
[David Kennedy](#)
- [C++ Committee felled by Concept virus](#)
[Nathan Myers](#)
- [Syntax completion - a bad thing?](#)
[Andrew Kelly](#)
- [Re: Mike Schlier on memory loss by cosmic radiation](#)
[Martin Minow](#)
- [Re: The *Shetland Times* Summary](#)
[John Pelan](#)

- [Maryland Recycles Law On "Annoying" E-Mail](#)
[AOP Bulletin via David Farber](#)
 - [Re: Electronic Funds Transfer without stealing PIN/TAN](#)
[Dan Wallach](#)
[Lloyd Wood](#)
 - [Re: Student takes 3.5 hours to crack RC4 40-bit key](#)
[D. Dale Gulledge](#)
 - [Proposed satellite monitoring of car movements in Sweden](#)
[Feliks Kluzniak](#)
 - [Car radio "security" KeyCodes](#)
[Paddy Spencer](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✶ **The (f)e-mail of the PCs is more deadly than the bail [!]**

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

Thu, 6 Feb 97 10:31:37 PST

The case involving Adelyn Lee and Oracle's CEO Larry Ellison (see [RISKS-18.07-08](#)) resulted in Ms. Lee being found guilty of perjury and falsification of evidence. She had previously won a \$100,000 settlement against Oracle, using as evidence an e-mail message ('`I have terminated Adelyn per your request.``') supposedly sent to Ellison by her former boss, Oracle VP Craig Ramsey. The prosecutor claimed that Lee had sent the message herself from Ramsey's account. She faces up to four years in jail. Subsequently, the judge ruled that she may not use any of that settlement money to pay her bail. [Source: *San Francisco Chronicle*, 29 Jan 1997, A11, and 31 Jan 1997, E1]

[... Another case involving the credibility of digital

evidence in
penetrable, tamperable, and spoofable environments...
Apologies to those
of you who do not know the classical poem from whose title the
Subject:
line takes off. PGN]

✦ Difficulties in developing large systems: IRS, etc.

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

Thu, 6 Feb 97 10:20:58 PST

The IRS is apparently going to abandon its past Tax Systems Modernization effort, on which it has spent \$4 billion. In testimony for the National Commission on Restructuring [``reinventing''] the IRS, IRS Assistant Commissioner Arthur Gross (who less than a year ago took on responsibility for IRS computers) stated that the systems ``do not work in the real world.'' (Past criticism has come from the Government Accounting Office and the National Research Council. See also [RISKS-17.96](#), 18.23-25, 18.43.) Gross noted that the IRS lacks the ``intellectual capital'' for carrying out the effort. One system had been cancelled earlier (the program for converting paper returns to electronic form), and 12 more systems are under review. Gross is proposing to contract out the processing of individual returns to commercial firms (which raises all sorts of privacy issues), although that is only a small portion of the processing demands. [Source: An item from *The New York Times*, seen in the *San Francisco*

Chronicle*, 31
Jan 1997, A1.]

A subsequent editorial on the IRS's plight [*Chron*, 2 Feb 1997] also reminds us that the FBI ``threw away'' a \$500-million fingerprint-on-demand computer and its crime information database, the State of California spent \$1 billion on its nonfunctional welfare database system, along with more millions on BART and the DMV. Readers of RISKS are well aware of the difficulties of developing large systems. The real question is whether anyone is learning from the past experience. If only we were building bridges and Henry Petroski were able to help us!

✶ E-mail saboteurs confuse Colombian kidnapping negotiations

Miranda Mowbray <mjfm@hplb.hpl.hp.com>
Mon, 3 Feb 1997 20:21:11 GMT

Last August, sixty Colombian soldiers were kidnapped by the Fuerzas Armadas Revolucionarias de Colombia (FARC), a Marxist-Leninist guerrilla group. The Colombian Government announced a few days ago that they would change from negotiating with the kidnapers through face-to-face meetings with intermediaries, which is slow and dangerous, to negotiating by e-mail.

Just after the announcement, the Government received a puzzled message from the FARC, saying that they had already received two e-mail messages claiming to be from the Government. The e-mails are thought to have come

from
right-wing saboteurs who do not want any negotiations to take
place.

Source: BBC World Service News, 2/2/97
Miranda Mowbray mjfm@hplb.hpl.hp.com

⚡ Dutch bank folly

Sape Mullender <sape@styx.huygens.org>
Mon, 03 Feb 1997 22:31:21 +0100

An interesting scandal concerning electronic banking occurred in
Holland.

It needs a bit of introduction: Banks have a system of 'direct
debit'
whereby a company (originally the utility companies, now almost
every
company that requires periodic payments for services) can
directly charge an
amount to a client's bank account. Clients have to agree to
this in advance
by signing a statement authorizing a company to do such direct
debits. The
banks guarantee that, up to three weeks after such a debit has
occurred, the
client can undo the transaction. Companies can use electronic-
banking
software on their PCs to carry out direct debits. The software
package
(Girotel) is the same as the one clients can use to do their
banking
electronically from their homes.

Last month, a Friesian church minister who publishes, I believe,
a magazine
of some sort, requested a direct-debit arrangement so that he
could directly

debit the accounts of his subscribers. He was vetted by the bank and declared reliable, so he got permission to carry out direct debit -- supposedly from consenting customers.

He then set to experimenting with it and discovered that he could direct-debit the account of his sister-in-law without her signed agreement and that he could also completely control the text on her bank statement (except for the amount and the bank-account number). He withdrew Hfl 2.50 from her account and got the text 'Waterleidingbedrijf Friesland' (Water utility company Friesland) on her bank statement.

Our minister was surprised and informed the press which led to some considerable outrage about bank security. A bank director, confronted with the situation said that 'nobody who had ever had money direct-debited from his account wrongfully has not gotten it back' (sorry about the double negative, but that's the way he put it).

The news programme in which he said this had just presented results from a poll that showed that 20% of the people interviewed never check their bank statements. One wonders how the bank discovers whether people who do not check their bank statement have had wrongful direct debits. The banks certainly appear to ignore the authorizations. The reporter, unfortunately, was not clever enough to ask the obvious follow-up question.

Sape Mullender

✶ Will-o'-the-w-ISP! More on AOL, Cyber Promotions

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

Thu, 6 Feb 97 9:47:20 PST

1. AOL's network bombed again, beginning at 2pm on 5 Feb 1997, and was not fully restored until about 4:30pm. The problem was attributed to a "technical glitch" in a software upgrade. [When have we heard that one before?]
2. AOL was inaccessible to new sign-ons for about 20 minutes on 2 Dec 1996, due to a ``software system bug'' in preparing for the influx of users expected when the flat-rate charges went into effect; the 165,000 existing sign-ons were left intact. After fixing the bug at 4:55pm, AOL then blocked about one of every 10 sign-on attempts for the evening. (We note this case retrospectively for the RISKS archives, although it may seem insignificant in light of more recent problems.)
3. Cyber Promotions Inc got dinged twice this week. On 3 Feb 1997, a federal court barred them from sending unsolicited e-mail ads to CompuServe's 5 million subscribers. The next day, a different federal court barred them from falsifying their FROM: addresses. [I presume CPI will still find ways to go through the (pro)motions.]

[Sources: Items 1 and 3 were in *San Francisco Chronicle* squibs, 6 Feb 1997. Item 2 was from *The Washington Post*, 3 Dec 1997, C3.]

⚡ AOL: 45 minutes and Out -- w/glitch

David Kennedy <76702.3557@CompuServe.COM>

03 Feb 97 00:37:44 EST

AOL's latest strategy: 45 minutes and out (via COMTEX Newswire 31 Jan 1997)

[Courtesy of the COMTEX Newswire via CompuServe's Executive News Service]

> PC Week Online (January 30, 1997) - America Online Inc.,
trying to
> alleviate its by now infamous network gridlock, has come up
with a new
> tactic: After 45 minutes on the service, users are being asked
to log
> off. If they don't respond in 10 minutes, their session is
ended. [...]
> But there's one catch: Certain games, such as an AOL contest
dubbed
> "Neverwinter," disguise the dialog box, resulting in users
being kicked
> off the system without warning, according to some disgruntled
subscribers
> and an AOL spokesman. [...] The Dulles, Va., company posted
a fix
> enabling users to view the dialog box in its AOL Insider area
earlier this
> week, he said.

Dave Kennedy [CISSP] Research Team Chief, National Computer Security Assoc.

⚡ C++ Committee felled by Concept virus

Nathan Myers <ncm@cantrip.org>

Tue, 4 Feb 1997 13:58:10 -0800 (PST)

At the November 1996 meeting of the ISO/ANSI C++ Standard committee, the computers provided by the meeting host for document preparation got an infection of the MS Word "Concept" macro virus. Since most attendees bring a laptop, those got infected too. We ended up spending twenty minutes in full committee (~60 people) on explanations of how to eliminate it, and protect against future infections. The Concept virus, by the way, got its big initial propagation aboard Microsoft Developer CDs.

Those of us who never use MS Word (because it's so buggy? see <http://www.cantrip.org/nobugs.html>) were tickled half to death. If a room full of C++ experts can't keep viruses off their machines, what hope is there for Joe User? (Those of us using Linux were, of course, unaffected.)

If ever there were grounds for a class action lawsuit against a software distributor, this would seem to be it: releasing a program with a virus susceptibility switch, with the switch defaulted to "on", and then negligently distributing a sample virus to take advantage of it. Given the great difficulty this has caused many large organizations (I gather the University of Oregon was severely disrupted) I would expect to see many co-plaintiffs on such a suit. (NB: IHNBAL*.)

The RISK? The usual: badly-designed software and arrogance lead to angry (or sometimes just embarrassed) customers, and lawsuits.

Incidentally, another RISK is causing users who know better than to run the buggy software laughing themselves silly at those who don't, and then

getting punched in the nose.

Nathan Myers <ncm@cantrip.org> (*) Nota Bene: I Have Never Been A Lawyer.

⚡ Syntax completion - a bad thing?

Andrew Kelly <andrewk@vsl.com.au>

Thu, 06 Feb 1997 08:14:57 +0900

Looking at Rational's Apex Ada development environment, I am not at all sure

I am 100% pleased with the syntax completion it performs. It seems to me

that syntax completion, as part of compilation, is not a good thing as it

repairs errors rather than report them (eg. unpaired begin/ends). The

obvious risk being that incorrect code will quite happily be "repaired"

(very possibly, incorrectly) and will compile successfully.

I believe syntax completion should be available during editing, but not

automatically employed during compilation. As far as I can discover, it

cannot be switched off in Apex either.

This seems, to me, to be more dangerous than it is useful ...

eg. If you

accidentally delete the "end" from a nested "if", where does the analyser

stuff the "end"? Indeed, even if it gets the placement correct (eg. by

inference from the indentation

Has anybody had any experiences with syntax completion that may confirm or allay my fears?

Andrew Kelly (andrewk@vsl.com.au), Software Design Engineer,

Vision Systems,
Technology Park, Adelaide, SA 5095, AUSTRALIA ph: +61-8-300 4602

✶ Mike Schlier on memory loss by cosmic radiation (Fischer, [RISKS-18.79](#))

Martin Minow <minow@apple.com>

Thu, 30 Jan 1997 15:46:38 -0800

> From: Mike Schlier <schlierm@wpos.hill.af.mil>
> To: Martin Minow <minow@apple.com>
> In [RISKS-18.79](#) you described an article describing research on
memory loss
> caused by cosmic radiation. I am in possession of a report
put out by the
> Boeing Corp titled "Single Event Upset In Avionics" detailing
a study of
> this same effect which was sponsored by the Defense Nuclear
Agency and the
> Naval Research Laboratory. This paper was submitted for
publication to the
> Dec 1992 IEEE Trans. Nucl. Sci.

> Mike Schlier, F-4 System Support, Hill AFB UT

[Ed Fischer <EdFischer@aol.com> remarked on a typo in Martin's
message,

``Summerized and translated by Martin Minow, minow@apple.
com''.

He suggested there must have been "Air[craft] conditioning".
PGN]

✶ Re: The Shetland Times Summary

John Pelan <johnp@am.qub.ac.uk>

Tue, 4 Feb 1997 17:59:25 +0000 (GMT)

PGN asked me to summarize an overwhelming number of contributions [some not included in RISKS, except for what was in [RISKS-18.64,78,79](#)] regarding the *Shetland Times* case.

The most significant point to note is that the court case has yet to happen. A judge has merely granted a temporary injunction ("interim interdict") preventing The Shetland News making hyper-text links to *The Shetland Times*, pending a full court case later this year. That decision was passed in October 1996 and no legal precedent has been set in doing so.

The case is being fought on the grounds of breach of UK Copyright Law. The final decision will probably rest on what constitutes a headline and whether the headlines in question can be treated as a separate work either individually or en masse, and whether websites fall within the definition of 'cable programme service' in the UK legislation.

At this stage the much touted implications of the outcome of the trial are highly speculative, often greatly exaggerated *and* are largely provisional on the complaint being upheld. Thus comments in this forum are best reserved at this stage, pending the actual trial and possible appeal, until the legal and technical RISKS, if any, become known.

John Pelan (J.Pelan@qub.ac.uk)

[Thanks to Mark Gould <Mark.Gould@Bristol.ac.uk> for additional comments.]

Definitive information available via <http://www.shetland-times.co.uk/>

and <http://www.shetland-news.co.uk/>]

✶ Maryland Recycles Law On "Annoying" E-Mail

David Farber <farber@cis.upenn.edu>

Tue, 04 Feb 1997 17:37:46 -0500

Excerpted from...

```
=====
AOP Bulletin           Friday, February 3, 1997           Volume 97:05
=====
```

The following is information distributed to members of the Association of Online Professionals and others involved in the online communications industry. Contacts and other information about AOP may be found at <http://www.aop.org>.

```
*****
Maryland Recycles Law On "Annoying" E-Mail
*****
```

A Maryland bill that would make it illegal to send "annoying" or "embarrassing" e-mail was introduced this week by Democratic General Assembly member Samuel Rosenberg.

The bill got little support when it was introduced last year, but Rosenberg hopes to play off of recent murders involving electronic mail to see the bill passed.

Civil liberties groups argue that the law would be unconstitutional, and

that the terms "annoy" and "embarrass" are too vague to be meaningful.

If passed, House Bill 778 would amend the state's criminal harassment law

to prohibit the use of e-mail to annoy, abuse, torment, harass, or

embarrass other people, with violators receiving a fine up to \$500 and three years in jail.

A similar bill introduced last year is quietly progressing through New

York's state legislature. Senate Bill 1414, introduced by Democratic State

Senator Ray Goodman, could be voted on in the House early this year.

Full text of the Maryland bill can be found at <http://mlis.state.md.us/1997rs/billfile/HB0778.htm>.

⚡ Re: Electronic Funds Transfer without stealing PIN/TAN

Dan Wallach <dwallach@CS.Princeton.EDU>

Mon, 03 Feb 1997 13:01:00 -0500

[Summary: an ActiveX control can add a pending online transfer to your Quicken file]

While interesting, this is a great example of "I told you so." When you accept an ActiveX control, you're allowing completely arbitrary code to rummage around your machine and do anything it pleases. That same code could make extremely expensive phone calls (900 numbers or whatever) with your modem; it can read, write, and delete any file on your computer; it can install Trojan horses and viruses. All without any of the

subterfuge and
hackery required to do it with Java. ActiveX hands away the
keys to your
computer.

That said, ActiveX still has its uses. On a corporate internal
network,
ActiveX is a nice replacement for custom internal applications,
where the
internal app would have been completely trusted, anyway.
ActiveX across the
Internet, however, is a disaster that doesn't have to wait
very long to
happen. The only security barrier is an annoying dialog box
that many users
will either ignore or configure away [one wrong click and you
now trust code
signed by each and every key issued by a given CA (e.g.,
VeriSign)].

The solution? Blocking ActiveX (or Java) at the firewall seems
fragile, at
best [see Dave Martin et al.]. Ideally you want to install your
security
policy [e.g., only allow ActiveX signed by your IS department]
inside every
user's Web browser. I can't speak for any browser vendors, but
it's safe to
suspect they're working on it.

Dan Wallach
Science Department
dwallach@cs.princeton.edu
[http://www.cs.princeton.edu/
~dwallach/](http://www.cs.princeton.edu/~dwallach/) PGP Ready

Princeton University, Computer
<http://www.cs.princeton.edu/>

**[⚡ Re: Electronic Funds Transfer without stealing PIN/TAN
\(RISKS-18.80\)](#)**

Lloyd Wood <eep1lw@surrey.ac.uk>

Thu, 6 Feb 1997 21:06:59 +0000 (GMT)

>
> From: weberwu@tfh-berlin.de (Debora Weber-Wulff)
> The newspaper quotes various officials at Microsoft et al.
> expressing disbelief

'We left that out of the third-party developer documentation!
Who leaked
it?'

> /outrage

'We've been beaten to market! By Germans! This is unamerican!'

> /"we're working on it".

'We'll be giving away our own secretly-siphon-all-your-money-to-Microsoft
ActiveX program, currently undergoing final usability tests and
stringent
quality assurance in our developer labs, at no cost to you -
just to try and
regain our deserved share of this exciting new emerging market!'

Where does your money want to go today?

L.

multiple mailing lists and resends to me.
if we had a decent newsfeed I'd've read it in comp.risks first.
<URL:<http://www.sat-net.com/L.Wood/>><L.Wood@ieee.org>+44-1483-
300800x3435

⚡ Re: Student takes 3.5 hours to crack RC4 40-bit key ([RISKS-18.80](#))

D. Dale Gullledge <ddg@cci.com>
Wed, 5 Feb 97 10:18:00 EST

Last night, in his State of the Union address, President Clinton advocated placing confidential medical data online, as well as getting schools connected to the Internet. So long as his administration is opposed to strong encryption and insistent on putting sensitive private information on the net, the risks are numerous. This contest offered a \$1000 prize. The price for specific data on the net probably runs much higher than that.

✈ Proposed satellite monitoring of car movements in Sweden

Feliks Kluzniak <feliks@carlstedt.se>

Wed, 29 Jan 1997 20:39:29 +0100 (MET)

The new issue of "Dagens IT", no. 3, dated 28 Jan - 3 Feb 1997 (a Swedish paper aimed at information technology professionals), contains an item that might be of some interest to those RISKS readers who followed discussions about automatic highway toll booths in the US and related subjects.

My (probably imperfect) translation follows.

Car users will be be put in "feetcuffs"
(written by Margaretha Sundstroem)

With the help of a new satellite system car users might pay different taxes, depending on when and where they drive. This is what the State communications commission is said to be discussing.

According to (the newspaper) "Dagens Politik", the State communications

commission is discussing a proposal to use satellites for determining car taxes in the future. It is proposed that all of Sweden's 3.5 million cars should be equipped with a little reader fastened to the instrument board. Car users would then buy cards that can be inserted into the reader. The card would communicate with a satellite that would register where you drive and for how long. The car tax would then be withdrawn from the card.

The proposal has been put forward by the State institution for communication analysis. They estimate that just the Stockholm (tax) authorities would be able to earn six billion crowns by using this system.

The costs for car users would thereby increase.

- - - -

The reference to "feetcuffs" (by analogy to "handcuffs" - ankle shackles?) is an allusion to radio transmitters that are irremovably fastened to the ankles of some criminals in this country so that the authorities can monitor their compliance with the rules of house arrest.

The word "communication" is meant to include car traffic etc. The word "billion" is given in its US meaning: a thousand million.

The risks? Apart from the risks of having very complex systems automatically determine how much you have to pay, there are the usual privacy considerations. Some cry out "big brother". Others say you are already in this situation if you carry a cellular phone.

Feliks Kluzniak, Carlstedt Research & Technology, Gothenburg

⚡ Car radio "security" KeyCodes

Paddy Spencer <paddy.spencer@parallax.co.uk>

Tue, 04 Feb 1997 12:41:30 GMT

Some time ago I managed to run the battery down on my car and after getting a jump start I found the radio, instead of displaying the station frequency showed three bars (---) flashing. I didn't know what the hell this was about so started randomly pressing buttons (the radio has 4 pre-set station buttons) and found that buttons 1-3 changed the number but 4 didn't appear to do anything. Eventually the display stopped flashing and wouldn't accept any more button presses. I was bemused.

Lying awake that night I realised that this was of course the security system that Ford introduced into their audio systems: disconnect the power source (here done by running the battery flat) and you need to enter a security code to regain access to your system.

I asked around various Ford garages and eventually found one that offered to give me the code -- apparently there is a database of all security codes that is sorted by the serial code on the radio. I took it along and the guy quite happily took the radio off and dug out the code and told me what to do to set it; you get ten goes to put the right code in, after this you have to leave it in the car with the ignition on, but the engine not running for 1

hour, after which you get to try again.

So where are the RISKS?

1. I received about half a dozen different sets of instructions on how to reset the radio -- all from Ford staff! Introducing a technology throughout your entire product spectrum and not making sure your staff know how to use it...

2. The guy who found the code for me made no effort to ascertain that I had a legitimate right to own the radio or retrieve the code. For all he knew, I might have nicked it from a car that morning and be wanting to have it reset in order to sell it later.

3. After finding out the code, he then wrote it on the case of the radio -- on a label provided by Ford for this purpose! So Ford on the one hand say "If a thief removes the radio he can't use it because he doesn't know the code" and on the other they're saying "If you need to know the code just take the radio out and have a look on the case."

Not the most secure security system I've ever come across!

Paddy Spencer

Parallax Solutions Ltd (<http://www.parallax.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 18: Issue 82

Friday 14 February 1997

Contents

- [Does CNID really give you anonymity?](#)
[PGN](#)
- [48-bit RC5 bites the dust](#)
[PGN](#)
- [NASD loses records on 20,000 brokers](#)
[Stern](#)
- [Risks of technical illustrations](#)
[Bear R Giles](#)
- [NT Attacks](#)
[Christopher Klaus](#)
- [Hostile ActiveX Control demonstrated](#)
[Klaus Brunnstein](#)
- [More on the risks of ActiveX](#)
[Joe Meadows](#)
- [Digital cameras may explode](#)
[Mark Seecof](#)
- [Cell phones and car accidents](#)
[Edupage](#)
[13 Feb 1997](#)
- [Risk of IRS Outsourcing Processing](#)

[John Pescatore](#)

● [Re: Will-o'-the-w-ISP! More on AOL, Cyber Promotions](#)

[Sean Eric Fagan](#)

● [Re: Word virus/C++ committee](#)

[Andrew Koenig](#)

● [Re: Y2K? Y1990 strikes again!](#)

[Mark Brader](#)

● [Info on RISKS \(comp.risks\)](#)

⚡ Does CNID really give you anonymity?

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

Fri, 14 Feb 97 11:02:50 PST

>From the time of an upgrade on 1 Jan 1997 until 26 Jan 1997, the mechanisms that are supposed to block the Calling Number ID (misnamed Caller ID) service FAILED in the 510 and 415 areas codes. As many as 516 businesses with PBXs were able to obtain calling numbers despite presumed blocking. (Something on the order of 50% of the subscribers are rumored to have requested blocking.) [Source: *San Francisco Chronicle*, 14 Feb 1991. Watch out if you thought you were sending anonymous tele-valentines to companies with PBXs!]

⚡ 48-bit RC5 bites the dust

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

Fri, 14 Feb 1997 8:02:49 PST

In [RISKS-18.81](#), we noted that Ian Goldberg of U.C. Berkeley had cracked the 40-bit RC5 in 3.5 hours -- the first step in the RSA Data Security challenge posed on 28 Jan 1997. The second step was taken on 10 Feb 1997 by Germano Caronni, a graduate student at the Swiss Federal Institute of Technology. Caronni (with a lot of help from his friends) has recovered the key for text encrypted with 48-bit RC5, with the help of 3,500 computers and attaining an peak rate of 1.5 trillion keys searched per hour, over a period of 312 hours. A press release from RSA (given some circulation in the media) on gives some details. Close to the median expected effort, about 57% of the key space was exhausted. The Caronni team is now working on the next challenge, RC5-56. It is easy to clone yourself through virtual replication. [In this case, the team has a lot of Caronnis!]

✶ NASD loses records on 20,000 brokers

"Stern, just Stern" <stern@panix.com>

Fri, 7 Feb 1997 09:16:18 -0500 (EST)

The National Association of Securities Dealers (NASD) is the self-regulatory organization that oversees broker-dealers and their employees in the United States. It maintains a database of brokers and any disciplinary action taken against them, a database that the public can access by calling Disclosure, Inc. (1-800-638-8241 in the U.S.) It's a good idea before doing business with a new broker-dealer or a new broker to call Disclosure to

check if they
have been a problem for other investors in the past.

Unfortunately, the NASD has purged 20,000 records from their files.

According to the Associated Press,

The NASD said it inadvertently issued faulty guidelines telling clerks that "revised" rules allowed them to purge a broad range of disciplinary data from the central registration depository.

The risks are (at least) threefold. First, that investors will not have access to this valuable information and that people may deal with unscrupulous brokers as a result. Second, other regulatory agencies that rely upon the NASD's record will not be able to perform their functions.

Thirdly, the NASD itself will not be able to refer to past disciplinary records on these brokers in deciding penalties in response to new complaints.

The NASD believes it will be able to reconstruct its records in a couple of months.

✶ Risks of technical illustrations

Bear R Giles <bear@indra.com>

Fri, 14 Feb 1997 14:25:12 -0700 (MST)

In this month's Scientific American there is a section on the Internet.

The first full-page graphic has a flow-chart-like diagram over the user's monitor. One line near the top illustrates the risks of technical illustrations without careful review by a knowledgeable person:

(Conditional box)

"Already open for exclusive use and not the supper user?"

This error isn't as bad as the `_Dr Dobb's_` cover illustration of a "red-black" tree where the elements of the tree weren't sorted (*oops*), or another "photorealistic" depiction of a lightbulb that could never be screwed into any socket on this planet (due to the image being flipped during layout), but it's still enough for me to wonder how much care went into the other graphics in the article.

At least all of the countries in the European/middle Eastern map appear to be present. (Unlike a major newsweekly that attempted a very creative approach to regional peace a few years back. :-)

Bear R Giles bear@indra.com [Pay to the Bear-R? or the Bare "R"? PGN]

[I had to point out in my role as panel chair for the cryptographer's panel at the January 1997 RSA Data Security Conference that the artist who rendered the giant version of the standard RSA two-key logo had neglected to realize that the two keys were supposed to fit together. They did not.
PGN]

NT Attacks

Christopher Klaus <cklaus@iss.net>
Wed, 12 Feb 1997 09:54:26 -0500 (EST)

Summary of recent attacks that have become more well known.

These attacks have been discussed on NT Security mailing list but the knowledge about them has not spread widely outside of the security mailing list circle: NT CPU Port Attacks, NT DNS Denial Attack, NT Trojan Password DLL.

* NT CPU Port Attacks

On NT 3.51 and NT 4.0, there are TCP ports that are open that when an attacker connects to them, types in some random characters, and drops the connection, the CPU on the machine goes to 100% usage.

For example, connect to TCP port 135 (RPC server), type in "thiswilldoacpuattack" and disconnect. Then check the CPU usage. The CPU will be at 100% usage and the machine will be noticeably slower. It is possible to kill and restart the rpcss process to stop the CPU usage.

DNS (TCP port 53 & 65589) is susceptible to this attack as well. In 16-bits, port 65589 is port 53. $65589 = 0x10035$. $53 = 0x35$

Solution:

On NT 4.0, there is filter capability to block all TCP ports except needed critical ones. You may want to enable that.

There is a hotfix available on

<ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/hotfixes-postSP2/RPC-fix>

There is a DNS beta that fixed the random character on the port attack.

It is available via ftp from rhino.microsoft.com, log on as

DNSBeta with a password of DNSBeta. In the /service_pack3/x86 directory there is a file called DNS.EXE dated 1/26/97.

* NT DNS Denial Attack

If an attacker spoofs a response that the DNS never requested, DNS will terminate. There is an advisory on this available at <http://www.iss.net/lists/general/0118.html>

Solution:

Currently, Microsoft is working on a solution.

* NT Trojan Password DLL

On NT 4.0 and 3.51, there is some entries in the registry that point to a DLL that does not exist, that lets an attacker to put their own DLL in place. There is one DLL that will capture all password changes into a file, so an attacker can obtain any passwords that get changed pertaining to passwords residing on that machine. Ideally for an attacker, placing the DLL on a domain controller machine where most password changes can take place may produce the greatest amount of password information.

More information is available with source code for the password changer

DLL at: <ftp://ftp.iss.net/pub/lists/ntsecurity-digest.archive/v02.n114>

or Knowledge Base article <http://www.microsoft.com/kb/articles/q151/0/82.htm>

Solution:

To defend against this type of Trojan attack is to protect

access to your registry fiercely. A routine part of your security maintenance checks should be to take a close look at this registry key:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Lsa
\Notification Packages
```

Make sure that it does not contain any strange entries. NT 4.0 ships with a single entry to this registry key:

```
FPNWCLN
```

If anything else in this registry entry, find out what it is and whether or not it's needed. If not sure, remove the errant entry immediately. Netware requires the DLL, so if you already have installed the Netware DLL, then it should have been installed admin-writable only. If you do not have the Netware DLL installed, make sure the register entry is blank.

Acknowledgments

Thanks to the posters of the NT Security Mailing list where almost all of this information was derived. To subscribe, send e-mail to majordomo@iss.net and within the body of the message, type: "subscribe ntsecurity".

Christopher William Klaus, Internet Security Systems, Inc., 41
Perimeter
Center #660, East, Atlanta, GA 30346 <http://www.iss.net/> (770)
395-0150

⚡ Hostile ActiveX Control demonstrated

Klaus Brunnstein <brunnstein@rz.informatik.uni-hamburg.d400.de>
Tue, 11 Feb 1997 14:46:08 +0100

In a German TV show, 3 East German hackers (remotely linked to in/famous Chaos Computer Club) demonstrated how inherent risks of Microsoft`s ActiveX technology can expropriate naive users.

The hackers prepared a Web page attracting interest of surfers ("Becoming millionaire in 5 minutes"). When this Webpage was contacted via Microsoft`s Internet Explorer, an ActiveX control would be downloaded into the victims computer. This control would access Quicken (a program aimed at assisting electronic banking) to generate a transaction form to transfer some electronic cheque to some account specified by the hackers; this cheque would be trans- mitted with the next collective remittance. This may be the first "Hostile Control" which has been demonstrated in the public (btw: several Hostile Java Applets have appeared at several Internet sites; as such Hostile Applets as well as experiments with Java "viruses" have not been publicly displayed, the broad public tends to assume that Java Applets are "secure" :-).

According to some Microsoft expert, "all users should know" that ActiveX may have such side-effects which may include sniffing of disks as well as remote installation of software. A spokesman representing Microsoft Germany even suggested to disable ActiveX if the system is used for purposes of electronic fund transfer. Concerning general protective action against malign effects of ActiveX, Microsoft suggests using its ActiveX "certification" option: users should "only allow" remote access

from
"trustworthy" programmers. A 3-level scheme (low - medium -
high) of trust
is supported. On "high", only controls with an "authenticode"
are permitted;
no warning is given when such a code is detected. Any programmer
can buy his
authenticode for 20 dollar.

Any risk? No risk if you regard Microsoft or its affiliated
programmers as
"trustworthy".

Klaus Brunnstein (10 Feb 1997)

PS: concerning "trustworthiness": apart from many safety and
security
problems, users owe Microsoft the deployment of the first Macro
virus
(Concept.A), and the proliferation of several Wazzu`s which have
escaped
from several Microsoft CD- ROMs and WWW pages to the "interested
public". Users will experience major problems with enhanced
macro viruses to
work under Office 97, and users will see more platforms to be
attacked. Thanx to Microsoft :-)

More on the risks of ActiveX

Joe Meadows <joe.meadows@nobs.ca.boeing.com>
Sun, 09 Feb 1997 10:34:18 +0000

While the security community has fully recognized the risk of
accepting
controls from untrusted sources, it seems to have completely
ignored a
secondary risk of an existing control being subverted in
unexpected ways.
Perhaps all of the controls that come with MSIE are perfectly
safe, and

can't be subverted in any way (no buffer overflows, no mistakes), but it seems highly unlikely that all controls are written so perfectly.

Since one is basically giving away control of ones desktop to a web author by enabling ActiveX within a browser, many companies are avoiding the technology like the plague. Filtering it out at ones firewall is hardly effective, unless one were to parse through every HTML page and automatically remove the components that drive ActiveX (i.e. VBscript, the Object tag, etc). Not allowing ActiveX to be enabled in a web browser would seem to be a minimum requirement, not allowing browsers that support ActiveX would seem to be even better (and easier for a firewall implementation to handle - if the firewall sees that the user agent supports it, it could refuse to service it).

Until the vendor gives us more control over when/how a control gets used (not just control over when they get downloaded), I'll personally avoid the technology. I hope Dan Wallach's supposition that the vendors are working on it is true, but if they are, they're keeping awfully quiet about it (refusing to acknowledge that there even is a problem). Of course, that's nothing new. "Full disclosure" of security bugs has done more for improving security in the last few years than 20 years of discussion about "risks" has done (not to belittle the work done by the readers of this mailing list/newsgroup, I just wish vendors would recognize that todays risks are tomorrows exploits).

Joe Meadows [as always, usual disclaimers in risks.info apply]

⚡ Digital cameras may explode

Mark Seecof <Mark.Seecof@latimes.com>

Wed, 12 Feb 1997 17:40:48 -0800

Eastman Kodak Company has announced a product safety recall for some of its digital cameras because their battery packs overheat and rupture when charged. Only about 1900 "professional" cameras in the DCS 420 and 460, and AP NC 2000 series are affected. Kodak will handle replacement requests at (800) 698-3324 in the USA or through Kodak representatives overseas.

This is barely a computer RISK. Ordinary cameras usually have tiny batteries and no provision for connection to mains power. So long as "digital" means "using lots of electrical power" portable digital devices may pose physical risks that older technologies do not engender.

Mark S.

⚡ Cell phones and car accidents (Edupage, 13 Feb 1997)

<educom@elanor.oit.unc.edu>

Thu, 13 Feb 1997 13:35:26 -0500

Researchers at the University of Toronto say that drivers whose attention is

distracted while talking on a cellular phone are four times more likely to be involved in an accident. However, insurance companies do not plan to raise insurance premiums, because accident rates have not increased overall.

The researchers also found little difference between the use of a receiver or hands-free model of phone, indicating that the problem is one of mental, rather than physical preoccupation. (*Toronto Globe & Mail*, 13 Feb 97, A1; Edupage, 13 Feb 1997)

✦ Risk of IRS Outsourcing Processing

John Pescatore <johnp@tis.com>

Fri, 07 Feb 1997 14:17:06 -0500

In [RISKS-18.81](#) about the IRS axing the Tax System Modernization project, PGN added a parenthetical comment:

>>Gross is proposing to contract out the processing of individual returns to commercial firms (which raises all sorts of privacy issues), although that is only a small portion of the processing demands.<<

This has shown up elsewhere, I guess expressing a concern that if the IRS used commercial firms to process tax returns, the risks to taxpayer privacy might *increase.* This concern must flow from a belief that a government agency or employee is less likely to compromise the privacy of a return than would a private sector employee.

Of course, the government agency usually has a monopoly on processing and the government employee generally has little to fear as far as termination of employment due to inappropriate handling of sensitive materials. So, I think the motivation for meeting privacy standards is good deal stronger in the private sector.

>From a privacy perspective, I don't think too many of us would want a government agency preparing our tax returns, handling our checking account, or storing the records of counseling sessions - yet we routinely rely on commercial firms for those private matters.

The real risk of outsourcing such processing will be the realization that there are no defined policy/procedures/standards for what constitutes proper handling to maintain some level of privacy. If encryption is to be used, how strong? etc.

John Pescatore, Trusted Information Systems, 15204 Omega Drive, Rockville, MD 20850 johnp@tis.com 301-947-7153, 301-527-0482 (fax)

⚡ Re: Will-o'-the-w-ISP! More on AOL, Cyber Promotions ([RISKS-18.81](#))

Sean Eric Fagan <sef@Kithrup.COM>
Thu, 6 Feb 1997 20:19:02 -0800

>3. Cyber Promotions Inc got dinged twice this week.
federal court
>barred them from falsifying their FROM: addresses. ...

I assume the last one refers to the settlement between CP and AOL. That is, unfortunately, not what it said.

The settlement AOL and CP signed onto says that CP will not be legally barred from sending e-mail to AOL's customers, but that they may do so only from a specified list of domains (five domain names, to be precise). AOL customers who wish to receive these messages (and AOL people assure me that, strange as it may seem, there are some who do!) can do so by disabling the PreferredMail blocking system.

The benefit to AOL, of course, is that they will no longer have to update their list of blocked domains daily with whatever new domains CP came up with (some of which were not real, and some of which weren't even valid domains).

Cyberpromo delenda est!

✦ Re: Word virus/C++ committee (Myers, [RISKS-18.81](#))

Andrew Koenig <ark@research.att.com>
Mon, 10 Feb 1997 09:50:58 +0500

In [RISKS-18.81](#), Nathan Myers talks about a Word virus that apparently got loose during a recent meeting of the C++ standards committee.

I have a few more remarks to add:

1. At the time of the meeting, Microsoft had had a program

available for more than a year that would detect and remove such viruses. Nevertheless, only a few committee members had that program installed on their machines.

2. The present version of Word has automatic macro execution turned off by default, so such viruses cannot propagate without explicit user action.
3. Troff has had the capability for similar viruses for many years. I suspect that the reason it hasn't been a problem has been the relatively smaller number of users.

Once the existence of Word macro viruses became known, I think Microsoft acted reasonably promptly to make a defense available. Yes, they should have been aware of the possibility before that, but I think it's going a bit too far to say they deserve to be sued. Lots of software companies have done worse.

Andrew Koenig ark@research.att.com

⚡ Re: Y2K? Y1990 strikes again!

Mark Brader <msb@sq.com>

Sat, 8 Feb 97 20:19:23 EST

Never mind 2000, some people are still having trouble dealing with 1990.

A recent posting by Steve Lau in misc.transport.urban-transit refers to certain tickets used for combined travel on BART and Muni, two transit systems in the San Francisco area. Among other problems, he reports that:

> the machines that dispense them can't print dates beyond 12-31-89. All
> of the tickets come out dated 1987. Last year they came out dated 1986.

And, yes, on at least one occasion it was claimed that his ticket was ten years out of date!

Mark Brader, msb@sq.com, SoftQuad Inc., Toronto



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 18: Issue 83

Friday 21 February 1997

Contents

- [TCAS and the F-16 incidents](#)
[PGN](#)
- [B777 autopilot/flight-director problems?](#)
[Peter Ladkin](#)
- [Myths about digital signatures](#)
[Edward Felten](#)
- [Suit Over Computer Use](#)
[David Kennedy](#)
- [Bank Sued for Racist E-Mail](#)
[David Kennedy](#)
- [Computer glitch mails out multiple driver's licenses](#)
[Dave Tarabar](#)
- [Proprietary data formats and backcompatibility](#)
[Lloyd Wood](#)
- [Web banking](#)
[Harold Asmis](#)
- [Forgeries and Dejanews](#)
[Robert Ames](#)
- [Judge Shuts Down Another Cyberporn Scam](#)
[Edupage](#)

- [Who made the call in the Moldova porn scam?](#)
[Doug Claar](#)
 - [Virus mailed out on PhotoDisc CD-ROM](#)
[John C. Rivard](#)
 - [Y2K "problem" in virus?](#)
[Jim Griffith](#)
 - [Mobile code security mailing list](#)
[Edward Felten](#)
 - [ActiveX basic problem](#)
[Paul Robinson](#)
 - [MS on the CCC ActiveX virus](#)
[Tod Nielsen and Brad Silverberg via Lloyd Wood](#)
 - [Microsoft "defends" ActiveX](#)
[Travis Winfrey](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✈ TCAS and the F-16 incidents

"Peter G. Neumann" <neumann@csl.sri.com>
Thu, 20 Feb 97 11:03:13 PST

There have now been four recent incidents involving F-16s and commercial airliners with the TCAS automated collision avoidance system.

1. On 5 Feb 1997, two Air Force F-16s closed on a Nation's Air Boeing 727 passenger jet heading for JFK in NY. A TCAS alarm caused the 727 pilot to take evasive action, flooring three passengers and crew members. This occurred in a fairly large restricted area through which the 727 had been cleared to fly. One of the F-16 pilots had earlier identified the 727 as a passenger plane, but continued to chase it ``as an intruder into his airspace''. The instructor pilot told his trainee pilot to stay

out of the way ``till this, uh, bozo gets out of the airspace.'' He was eventually ordered to stop the chase, but ``the command may have been delayed because the fighter pilot was on the wrong frequency'' (according to the Air Force report).

2. On 7 Feb 1997, four Air National Guard F-16s from Andrews Air Force Base passed an American Eagle commuter plane bound from Raleigh to NY. Three of the F-16s were above the commuter plane, one below. A TCAS alarm caused the American Eagle pilot to take evasive action.

3. Also on 7 Feb 1997, two Air Force F-16s entered the safety zone around an American Airlines jet over Palacios TX.

4. Also on 7 Feb 1997, two Air Force F-16s entered the safety zone around an Northwest Airlines jet over Clovis, NM.

The Air Force insists that none of these cases was a close call (that is, with less than 500 feet separation), and that such close encounters have happened routinely in the past without causing concern -- before the advent of TCAS. So, we can chalk this up either as an indication that TCAS works (albeit too well?), or as a failure of the Air Force to understand the risks of false alarms in someone else's safety system!

[Sources: items in *The Washington Post* 8 Feb 1997, *Los Angeles Times*, 11 Feb 1997, A14, and *The New York Times*, 19 Feb 1997.]

✈ B777 autopilot/flight-director problems?

Peter Ladkin <ladkin@TechFak.Uni-Bielefeld.DE>

Tue, 18 Feb 1997 17:58:08 +0100

Flight International (19-25 Feb 97, p4) reports that the UK AAIB is looking into an uncommanded-rudder-movement incident on a British Airways Boeing 777-200A in October 1996. The B777 is a fly-by-wire (FBW) aircraft.

The aircraft departed Heathrow en route Jeddah, and was forced to turn back.

A UK CAA Occurrence Report talks of uncommanded movement of rudder and rudder pedals during climb and cruise, at random intervals. The flaperons were also observed to move, it is surmised in counterresponse to the rudder movements. "Large rudder input" was required on the landing. An intermittent fault in the two autopilot/flight-director computers is suspected, and they're being lab-tested -- as are the rudder backdrive actuators.

It's perhaps important to point out the difference between the flight management system (FMS), of which the autopilot/flight-director is part, and the aircraft control system. The term 'fly-by-wire' is used by aerospace engineers (but not usually journalists) to refer to digital-computer operation of the control system. Many non-FBW aircraft, some which have been in service for 14 years now, have digital computer-controlled FMS's. In this B777 incident, FMS problems are suspected (but not yet confirmed), whereas control-system problems are not.

Peter Ladkin

✶ Myths about digital signatures

Edward Felten <felten@CS.Princeton.EDU>

Wed, 19 Feb 1997 17:12:43 -0500

There has been a lot of public discussion lately about digital signatures on mobile code. Several myths permeate this discussion. I'd like to puncture three of them.

* Myth 1: Digital signatures let you know who wrote a program, or where it came from.

Reality: Anybody can remove the author's signature or add their own signature. At best, a signature tells you that the signer endorsed the program recently. Endorsement is more useful than authorship anyway; most people care more about whether their corporate MIS department has endorsed a program than about who wrote the program.

* Myth 2: If X has signed a program, and I trust X, then it is safe for me to download the program.

Reality: There have been plenty of incidents of reputable and well-meaning organizations spreading viruses or serving as the base for security attacks. Before accepting a download from X, it's not enough to ask "Do I trust X?" One must also ask questions like "How carefully has X managed

his cryptographic keys?" and "What is the probability that X's security has been penetrated?"

* Myth 3: Digital signatures provide accountability; if a program signed by X is malicious, the victim can sue X.

Reality: Suppose I accept a download signed by X. A few seconds later there is some mysterious network traffic and then my disk gets wiped clean.

X could be the culprit. Or X could be innocent --- that code I downloaded from Y three days ago could have waited a while before detonating. Or somebody could have exploited a bug somewhere else in my system. I have *no evidence* to distinguish these cases --- all the evidence disappeared when my disk was erased. (We can assume the attacker is smart enough to remove the hostile code from his site immediately after the attack.)

If the attacker doesn't erase my disk, I can't trust the apparent evidence anyway. After all, the attacker had free run of my system and could have planted whatever "evidence" he liked. The evidence, whether real or not, will collapse in the first cross-examination.

Signatures can provide accountability, but only with much more rigorous logging and auditing than today's consumer software provides.

Suit Over Computer Use

David Kennedy <76702.3557@CompuServe.COM>
18 Feb 97 22:00:21 EST

Courtesy of United Press International via CompuServe's
Executive News Service:

UW prof accused of copying porno pics (UPI US & World, 13 Feb
1997)

> MADISON, Wis., Feb. 13 (UPI) -- The University of Wisconsin-
Madison is
> facing (Thursday) a sexual harassment lawsuit, claiming a
former medical
> professor used campus computers to copy hundreds of
pornographic pictures
> from the Internet.

Another employee is suing because the professor propositioned
her.

DMK Comment: Privacy fanatics balk when companies claim
privilege over the
contents and uses of the systems the companies own. In this
case, the
university is being held responsible for the actions of one of
their
employees. Given the academic-freedom environments in most
(all?) American
Universities (and probably elsewhere), the university is in a no-
win
position.

Dave Kennedy [CISSP] Research Team Chief, National Computer
Security Assoc.

⚡ Bank Sued for Racist E-Mail

David Kennedy <76702.3557@CompuServe.COM>
19 Feb 97 21:00:09 EST

Courtesy of the Dow Jones News Service via CompuServe's

Executive News Service:

Citibank Workers File Bias Lawsuit Over Racist E-Mail (Dow Jones, 18 Feb 1997)

By Frances A. McMorris
Staff Reporter of The Wall Street Journal

> NEW YORK -- Two black employees of the Citibank NA unit of Citicorp filed
> a race discrimination lawsuit after racist jokes were allegedly sent via
> electronic mail by several bank supervisors. The e-mail was identical to a
> set of racially charged jokes at the center of a lawsuit against Morgan
> Stanley & Co.

> The plaintiffs, Alvin Williamson, a vice-president, and Brenda Curtis, a
> secretary, contend that several Citibank supervisors, including vice-presidents, spread the offensive e-mail to specific colleagues around
> the country. The e-mail created a "pervasively abusive racially hostile
> work environment," the plaintiffs said in their lawsuit.

:: Mail sent on Jan 28th. Suit claims little or no action was taken against those who spread the message, although the company acknowledged an incident did take place and it was "putting into effect disciplinary actions" against the perpetrators.

DMK Comment: Another company is being sued for objectionable content of employee computer use.

Dave Kennedy [CISSP] Research Team Chief, National Computer Security Assoc.

⚡ Computer glitch mails out multiple driver's licenses

Dave Tarabar <dtarabar@systemsoft.com>

Thu, 20 Feb 1997 09:02:54 -0500

The Boston Globe, 20 Feb 1997, has a picture of a woman holding six copies of her new driver's license which came in the mail on the same day.

Two years ago, the Massachusetts Registry of Motor Vehicles converted to a new state-of-the-art system for producing driver's licenses. When a person renews a license, a digital color picture is taken. You are given a temporary paper license and are told that your permanent license will arrive shortly in the mail. The permanent license is a single piece of plastic (like a credit card). It should be more tamper-resistant than previous licenses, which had a Polaroid picture laminated to paper. So far there have been no reported problems with the system.

It appears that in certain cases, the system was spitting out multiple copies of a license and mailing them on the same day. A spokesman for the Registry says that a computer programming error has been identified and fixed. The Registry says that about 50 people reported receiving multiple licenses. The major Risk here is that extra licenses could be sold (or stolen) for the purpose of false IDs.

Another feature (or risk?) of the digital photographs is that it is no longer necessary to go in person to the Registry when renewing

your license
or replacing a lost or stolen license. You can just send a
check.

For many people, the most serious risk is that there is no
longer only one
copy of their driver's license picture :-)

Dave Tarabar, SystemSoft Corp., 2 Vision Drive Natick, MA 01760
dtarabar@systemsoft.com 1-508-647-2952

⚡ Proprietary data formats and backcompatibility

Lloyd Wood <L.Wood@surrey.ac.uk>
Wed, 19 Feb 1997 16:25:36 +0000 (GMT)

>From the Electronic Telegraph, Connected Newsbytes, Tuesday 18
Feb 1997:

Microsoft says that it has solved the problem of forward
compatibility - the way that old word processors can't read
documents produced by newer versions of the same software.
Apparently, if you're still using Office97 10 years from now
and
someone sends you an Office2007 file, your computer will lead
you
on to the Web to download a converter utility.

There are a number of risks inherent in this (assuming a network
connection,
assuming that the web hasn't undergone a sea change to a
completely
different access protocol), but these risks are experienced by
you, the user
of software that writes its data in a proprietary, publically
undocumented,
format that leaves you nothing else to fall back on.

In fact, these risks will encourage you to upgrade Office (or
Acrobat's

'portable'-document-format pdf reader, say) regularly to avoid them. Is this the best way forward?

L.

Software marketing - so good it's almost criminal.

<URL:<http://www.sat-net.com/L.Wood/>><L.Wood@ieee.org>+44-1483-300800x3435

Web banking

Harold Asmis <harold.w.asmis@hydro.on.ca>

Thu, 13 Feb 1997 12:37:30 -0500

Problem: Quirks in either our Corporation's implementation of caching or in other sites' interpretation of how caching works, has allowed the ability for complete strangers (in the organization) to view your confidential bank accounts.

Two weeks ago, we were setting up My Yahoo (a customized web page) for somebody (strictly technical news :). After setting up, we were quite surprised to get somebody else's web page. Ha, ha we thought, and it never happened again.

Now I've been informed that somebody was checking their Bank of Montreal web bank account. This is fairly heavily protected by user name and password.

Lo and Behold, he came up with somebody else's (in the organization) bank account! This fellow almost came to blows accusing that person of using his

PC at night! :)

What is happening here? I believe that MBANX is probably being slack about caching and the use of common IP firewalls, but we are probably caching something that shouldn't be cached.

Until this is resolved, I recommend that web accounts be only checked at home.

Harold W. Asmis harold.w.asmis@hydro.on.ca 1-416.592.7379 fax 416.592.5322
[Disclaimers]

Forgeries and Dejanews

Robert Ames <amesr@interlog.com>

Mon, 17 Feb 1997 08:21:44 -0500

It seems that an effective way to attack an individual is to forge a Usenet article purportedly from that person, and to include in the article "admissions" or bigotted statements which would reflect poorly on his character. The forged article is then collected by Dejanews and similar organizations and archived. It becomes part of the Dejanews "profile" on the supposed author.

I was one of the victims of a series of forgeries in August and September, 1996. The perpetrator originated at ixc.net in New York, and then telnetted to news.uu.net and other open news servers to post as the victim. Although I cancelled the forged article and posted a PGP-signed

repudiation, the article was still archived at Dejanews, and was recently used by someone to "prove" that I had made statements which put me in a bad light.

Since this is a general problem which can impact on anyone, I feel it needs to be discussed. Perhaps news archivers should be under the same scrutiny as credit reporting agencies.

⚡ Judge Shuts Down Another Cyberporn Scam (Edupage, 20 February 1997)

<educom@elanor.oit.unc.edu>

Thu, 20 Feb 1997 15:40:44 -0500

A federal district judge in New York has shut down an operation that lured pornography-seekers into visiting Web sites that surreptitiously dialed a telephone number in Moldova in the former Soviet Union, running up exorbitant long-distance phone charges. The scam is similar to several others which have been uncovered in recent months. A Web surfer is enticed to visit sites with names such as sexygirls, beavisbutthead, and ladult, which promise "All Nude All Free Pictures" and require that a special "viewer" must be downloaded to review the images. However, the viewer contains software that turns off the user's local connection to an Internet Service Provider and silently dials the number in Moldova. The Federal Trade Commission says this is "one of the most insidious scams" it has ever

seen. (*The New York Times*, 20 Feb 1997; Edupage, 20 February 1997; see [RISKS-18.80](#) for the earlier story.)

[A similar Reuters item was noted by Avi Rubin <rubin@research.att.com>.

PGN]

⚡ Who made the call in the Moldova porn scam?

Doug Claar <dclaar@hprtnyc.ptp.hp.com>

Thu, 20 Feb 1997 00:35:44 -0800

The San Jose Mercury News online service, discussing the Moldova porn scam, has two conflicting quotes, which raise an interesting question: Who is responsible? According to the article, The director of the FTC's Bureau of Consumer Protection, says "The defendants in this case are using software to hijack the computer's modem", which implies the defendants (who provided the trojan program) are at fault.

Later on, the article quotes AT&T's security manager, Richard Petillo, who said that the customers who were victimized are expected to pay their bills because "The subscribers actually made the calls and it would be unfair to other subscribers to offer those people the option of not paying the charges." So AT&T claims that the users are at fault, though they clearly have a good reason to take that position, since they'll have to pay if the customers don't.

Equating common sense and legal reality is always chancy, but if you steal my car and commit a crime, I don't *think* that I would be found to be at fault. But if you steal my phone line, AT&T thinks I'm at fault.

Doug Claar

✶ Virus mailed out on PhotoDisc CD-ROM

"John C. Rivard" <jcr@mcs.com>

Wed, 19 Feb 1997 15:29:56 -0600

PhotoDisc Inc. (<http://www.photodisc.com>) sells digital stock photography.

They send out CD-ROM discs to their customers that contain mostly low-resolution images that can be used for comping during page layout. You

pay to receive the high-resolution version for final production.

The discs

can be read on Macintosh and Windows machines, and also includes an image

browser/catalog program, as well as Adobe Acrobat 3.0 (used to read the included documentation).

Volume 4 of this disc arrived last week. Today I received a snail-mailed

letter dated February 13, 1997 from Tom Hughes, President of PhotoDisc Inc.,

RE: "Problem discovered with Acrobat Reader Software on Comping Disc 4." It

is directed to Macintosh users only, and warns against launching the Adobe

Acrobat software on this disc, because it is "corrupt" and "may result in

system file difficulties." The letter continues, "If you use an antiviral

utility, chances are good it's already caught the problem."

In the "unlikely event" that you have already "installed" Acrobat 3.0, the company has provided a downloadable utility (<http://www.photodisc.com/solution>) that can "rid your computer of all corrupt files." This "utility" is John Norstad's excellent freeware Macintosh anti-virus program, Disinfectant.

Of course, the problem isn't "corruption" at all; PhotoDisc distributed an application infected with a virus, specifically MBDF B, a virus that has been in the wild since at least February 1992. This virus, according to the Disinfectant documentation, can spread and infect both applications and system files.

I applaud PhotoDisc for taking prompt action, both in warning their users and in sending a replacement disc.

However, I question their vagueness about and apparent unwillingness to admit the true nature of the problem in their warning letter. Nowhere in this letter does the word "virus" even occur.

I also have to fault them for not understanding and communicating correct information about the problem: contrary to instructions in their letter and on their web site, your system CAN be infected without installing or copying the infected application. In fact, simply running Acrobat from the CD ROM will infect the System file on the user's machine.

It's an old RISK: scan your golden master for virii! (And this was a really OLD and well-known virus: Any Mac anti-virus software released

in the last
four years would have caught this.)

PhotoDisc recommends destroying Comping Disc 4 if you use a
Macintosh. They
will be sending a "clean, safe replacement disc" to all users,
Windows
included, next week. This disc will also include Disinfectant.

John C. Rivard <http://www.mcs.net/~jcr/> mailto:
jcr@mcs.com

⚡ Y2K "problem" in virus?

Jim Griffith <griffith@netcom.com>
Thu, 20 Feb 1997 17:10:25 -0800

Has anyone bothered to look and see if the Michaelangelo virus
will be
bitten by the Y2K problem? One can only hope...

Jim

[How many virus creators are concerned with good
software engineering practice? Or does it matter? PGN]

⚡ Mobile code security mailing list

Edward Felten <felten@CS.Princeton.EDU>
Wed, 19 Feb 1997 19:58:39 -0500

We are starting a moderated mailing list to discuss security
issues relating
to mobile code systems like Java, ActiveX, and JavaScript. To
join, send
e-mail to majordomo@cs.princeton.edu; your message body should

contain the
single line

"subscribe secure-mobile-code"

or if your desired TO: address is different from your FROM:
address,

"subscribe secure-mobile-code" (append your TO: address here)

⚡ ActiveX basic problem

Paul Robinson <foryou@erols.com>

Wed, 19 Feb 1997 13:33:51 -0500

As it has been pointed out in **Dr. Dobbs' Journal**, an ActiveX control is no less than a Windows Dynamic Link Library (DLL) that has all the power and capability of any other DLL loaded on a Windows system, i.e. any damn thing it wants to do.

This alone should ring the death knell on use of ActiveX for anything other than perhaps on an intranet behind a firewall that does not allow any incoming traffic, and maybe not even then.

Paul Robinson, Evergreen Software

⚡ MS on the CCC ActiveX virus (fwd)

Lloyd Wood <L.Wood@surrey.ac.uk>

Fri, 21 Feb 1997 16:06:20 +0000 (GMT)

Here is Microsoft's official line on the security of ActiveX.

This leaves a very nasty taste in my mouth. The onus on the users to be responsible with their tools, as usual, rather than on the developers to create safer tools. Lloyd

<URL:<http://www.sat-net.com/L.Wood/>><L.Wood@ieee.org>+44-1483-300800x3435

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

Date: Fri, 21 Feb 1997 10:31:18 -0500
>From: glen mccready <glen@qnx.com>
Subject: MS on the CCC ActiveX virus
Forwarded-by: garman@phs.k12.ar.us (Jason Garman)
>From: Site Builder Network <sbn@MICROSOFT.COM>
Subject: SBN Wire: News Flash

Dear Site Builder Network Member,

Tomorrow, Microsoft will be posting the attached letter to our web site, and sending it out to the Internet Explorer community. In it, Brad Silverberg addresses head-on the recent security questions facing the industry regarding malicious, unsigned controls. We know this issue is important to you and your customers, and wanted to give you a heads-up.

For more information, check out <http://www.microsoft.com/security>

Tod Nielsen, General Manager, Developer Relations Group

= = = = =
= = =

>From the Office of Brad Silverberg
Senior Vice President
Microsoft Corporation
1 Microsoft Way
Redmond, WA 98052

Dear Internet Users Everywhere:

You may have heard reports about a malicious software program created and demonstrated recently by the Chaos Computer Club (CCC) in Hamburg, Germany. I want to personally assure you that Microsoft(R) Internet Explorer 3.0 has the appropriate safeguards to protect against this type of threat. By using its default security level (High) that comes pre-set, Internet Explorer 3.0 will not download and run any "unsigned" control such as the one from the CCC.

The CCC demonstrated its malicious executable code running on Microsoft Internet Explorer 3.0, though they could just as easily have demonstrated a similar attack on any other browser. While it is unfortunate that hackers have created this harmful program, it does point out the need for users to act cautiously and responsibly on the Internet, just as they do in the physical world.

Malicious code can be written and disguised in many ways - within application macros, Java(tm) applets, ActiveX(tm) controls, Navigator plug-ins, Macintosh(R) applications and more. For that reason, with Internet Explorer 3.0, Microsoft has initiated efforts to protect users against these threats. Microsoft Authenticode(tm) in Internet Explorer 3.0 is the only commercial technology in use today that identifies who published executable code you might download from the Internet, and verifies that it hasn't been altered since publication.

If users choose to change the default security level from High to Medium, they still have the opportunity to protect themselves from unsigned code. At a Medium setting, prior to downloading and running executable software on your computer, Microsoft Internet Explorer presents you with a dialog either displaying the publisher's certificate, or informing you that an "unsigned control" can be run on your machine. At that point, in either case, you are in control and can decide how to proceed.

As you know, Microsoft is committed to giving users a rich computing experience while providing appropriate safeguards. Most useful and productive applications need a wide range of system services, and would be seriously limited in functionality without access to these services. This means that many Java applications will have to go "outside the sandbox" to provide users with rich functionality. By signing code, a developer can take advantage of these rich services while giving users the authentication and integrity safeguards they need. Other firms such as Sun and Netscape are following our lead, and have announced that they will also provide code signing for Java applets. Microsoft will also be providing an enhanced Java security model in the future, giving users and developers flexible levels of functionality and security.

Microsoft takes the threat of malicious code very seriously. It is a problem that affects everyone in our industry. This issue is not tied to any specific vendor or group of people. All of us that use

computers for work, education, or just plain fun need to be aware of potential risks and use the precautions that can insure we all get the most out of our computers. For this reason, we are committed to providing great safeguards against these types of threats in Internet Explorer. We expect hackers and virus writers to get increasingly sophisticated but we pledge we'll continue to keep you and us one step ahead of them.

Brad Silverberg

P.s. Be sure to check out our Web Executable Security Advisor at <http://www.microsoft.com/security>

Microsoft "defends" ActiveX

Travis Winfrey <travis@lombard.com>

Thu, 20 Feb 1997 10:43:36 -0800

The site <http://www.news.com/News/Item/0,4,8096,00.html?latest> discusses the MS response to the activeX/quicken bug where downloaded activeX applets can actually transfer real money out of your bank account (bug not applicable in America). They point to this URL:

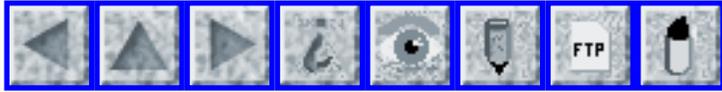
<http://www.microsoft.com/security/>

which has this instant-classic paragraph, emphasis not in the original:

While the Java sandbox enforces a high degree of security,
it does not let users download and run exciting multimedia
games or other full-featured programs on their computers.

As a result, users may want to download code that has full

access to their computers' resources.



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 18: Issue 84

Friday 21 February 1997

Contents

- [Highly classified files copied by Croat teens?](#)
[PGN](#)
- [Windows 95 will crash in 2038!](#)
[David Perrell via Chuck Wozniak](#)
- [Year 2K and my VCR...](#)
[Nicholas C. Weaver](#)
- [Downloading UPS-captured Signatures](#)
[Sharif Torpis](#)
- [Re: Myths about digital signatures](#)
[Theodore Y. Ts'o](#)
- [Re: MS on the CCC ActiveX virus](#)
[Fred Cohen](#)
[Steve Kilbane](#)
- [ActiveX - a real world view](#)
[John Pettitt](#)
- [ActiveX exploitation code in iX 3/97](#)
[Thomas Koenig](#)
- [Re: Bank Sued for Racist E-Mail](#)
[Jon Seymour](#)
- [Re: Who made the call in the Moldova porn scam?](#)

[John Kohl](#)

[Marc Horowitz](#)

 [Info on RISKS \(comp.risks\)](#)

Highly classified files copied by Croat teens?

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

Thu, 20 Feb 97 19:30:43 PST

Dave Farber <farber@cis.upenn.edu> noted a 19 Feb 1997 Reuter report from Zagreb indicating that 3 Croatian teenagers apparently broke Pentagon protection codes on the Internet and copied classified files from the Anderson nuclear installation and an unnamed satellite research center.

``The damage caused by the teenagers' destruction of high-profile protection programs could reach half a million dollars,' according to the Zagreb daily, *Vecernji List*. The three youths attend a special Zadar math-science school. ``Principal Zdravko Curko said the three had no criminal intent and their `success' was a compliment to their education.''

[PGN Abstracting]

Might we suspect that the files were actually unclassified, that the \$.5M is overblown, and that the breakins did not require much high-tech attacks?

[Are they just looking for something to Cro-at?]

Windows 95 will crash in 2038!

<Chuck_Wozniak@quantumdata.com>

Tue, 17 Dec 96 08:30:19 -0800

Accidental Year 2096 in e-mail message crashes Navigator w/ Win 95

The following was posted to two HTML related mail lists. The individual had his computer date accidentally set to 2096. Any mail that he sent or posted to a news group would crash the reader's computer if they were running Netscape Navigator Mail under Windows 95. The entire content, with headers, is supplied below.

Chuck Wozniak, Applications Engineer, Quantum Data, Inc.

- - - - -

Date: 11/25/96 7:59 AM
>From: "David Perrell" <davidp@earthlink.net>
Subject: Sorry if you crashed (W95 FYI: Chaos in 2038!)

It was brought to my attention that my posts to these lists have caused Netscape Mail running on Win95 to crash. I tried to test this by sending myself a message but was unable to run NS Mail at all.

I'm glad to say I found the problem: In the course of a HD upgrade my system clock had somehow built a 100-year bridge to the 21st century and was set to 2096. Subsequent testing shows that dates beyond 2038 cause many unwanted side effects in Win95, including the aforementioned crashes when NS Mail receives a message so dated.

Having returned to the present, I retrieved my previously sent test message dated 2096, and, sure enough, NS Mail crashed.

Sorry if anyone experienced this problem. It was not intentional.

(Also sorry that I rewrote/resent a 'transparent text' post on www-style. I thought one of these crashes had trashed the message.)

David Perrell

⚡ Year 2K and my VCR...

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

Fri, 21 Feb 1997 10:23:24 -0800 (PST)

As one of the few people who actually PROGRAMS his VCR, it came as a shock to me the realization that this piece of electronics (roughly two years old) will fail in the year 2000. One wonders how prevalent this problem is, in embedded systems shipping today. And I doubt there will be a bug fix for my VCR.

Nicholas C. Weaver nweaver@cs.berkeley.edu

[Are you talking about something that will fail only at midnight, or forever after the midnight turnover going into 1 Jan 2000? Furthermore, do you think the VCR makers are creative enough in their planned obsolescence to realize that this might be a nice way to induce you to buy a new VCR? PGN]

⚡ Downloading UPS-captured Signatures

Sharif Torpis <storpis@redhead.pbi.net>

Tue, 18 Feb 1997 13:15:59 -0800 (PST)

>From a UPS ad in the Feb 1997 Wired:

Once a signature is captured and downloaded to our mainframe, you can use

UPS OnLine Tracking Software to view it. You can even print it. To get the

software, just call 1-800-XXX-XXXX or visit our web site at www.ups.com.

Sure, we've all known about the capturing ever since UPS started doing it,

but now malicious users can add this to their toolbag. The more things

change the more they stay the same.

Sharif Torpis (storpis@pbi.net), Network Engineering, Pacific Bell Internet

🔥 Re: Myths about digital signatures (Felten, [RISKS-18.83](#))

"Theodore Y. Ts'o" <tytso@MIT.EDU>

Fri, 21 Feb 1997 16:31:27 -0500

* Myth 2: If X has signed a program, and I trust X, then it is safe for me

to download the program. [...]

Ed, It's even worse than what you described. Even if X has carefully

managed his cryptographic keys, and X's security hasn't been penetrated, X

might not have designed the component carefully, or have executed a

competent implementation of that design.

For example, if an Active X component has a loophole where (with

the right document) said component can be induced to interpret and execute arbitrary Visual Basic statements, even if the signer was honest, and legitimate, and properly went through all of the Microsoft certification procedures, it still might be possible to exploit a security bug in the Active X component. The Java security model at least **thinks** about this issue, where as the Active X approach completely punts about this concern.

So this is a double-edged RISK, combining the RISK of people not understanding what the digital signature means, and the RISK of more and more complex applications with powerful macro facilities being used in interesting ways (the prime example being the Word concept virus; the demarkation between code and data can get awfully blurry!).

Both of these RISKS aren't new ones, but when combined with the web and the automatic downloading of Active X components, the potential for problems caused by this combined set of RISKS is quite scary and sobering.

- Ted

⚡ Re: MS on the CCC ActiveX virus ([RISKS-18.83](#))

Fred Cohen <fc@ca.sandia.gov>
Fri, 21 Feb 1997 11:46:11 -0800 (PST)

Re: SBN Wire: News Flash, Brad Silverberg

> You may have heard reports about a malicious software program created and

> demonstrated recently by the Chaos Computer Club (CCC) in
Hamburg, Germany.
> I want to personally assure you that Microsoft(R) Internet
Explorer 3.0 has
> the appropriate safeguards to protect against this type of
threat. By using
> its default security level (High) that comes pre-set, Internet
Explorer 3.0
> will not download and run any "unsigned" control such as the
one from the
> CCC.

I appreciate your insightful opinion on this matter, however...
Anyone can get a signature key without authenticating their
legitimacy. It's relatively easy to break into a system
and take a
legitimate key. The default may be changed by the user
for one use
and remain changed. Other flaws in Explorer may be used
to turn
that feature on - then look out.

> The CCC demonstrated its malicious executable code running on
Microsoft
> Internet Explorer 3.0, though they could just as easily have
demonstrated a
> similar attack on any other browser. While it is unfortunate
that hackers
> have created this harmful program, it does point out the need
for users to
> act cautiously and responsibly on the Internet, just as they
do in the
> physical world.

I appreciate your insightful opinion on this matter, however...
This is not accurate. The very nature of ActiveX makes it
impossible to operate it securely. Unlike other vendors who
make attempts at providing improved protection, ActiveX is a
hole waiting to be exploited.

> Malicious code can be written and disguised in many ways -
within
> application macros, Java(tm) applets, ActiveX(tm) controls,

Navigator

> plug-ins, Macintosh(R) applications and more. For that reason, with
> Internet Explorer 3.0, Microsoft has initiated efforts to protect users
> against these threats. Microsoft Authenticode(tm) in Internet Explorer 3.0
> is the only commercial technology in use today that identifies who published
> executable code you might download from the Internet, and verifies that it
> hasn't been altered since publication.

I appreciate your insightful opinion on this matter, however...

No disguise is needed for malicious ActiveX programs. Any ActiveX
program can potentially - either maliciously or by accident or even
as a result of configuration differences, cause a system crash, the
corruption or destruction of information and/or unlimited leakage
and it doesn't depend on some hard-to-find hole in an otherwise
secure application. It is a direct result of the methods used by
Microsoft, cannot be easily cured with any bug-fix.

> If users choose to change the default security level from High to Medium,
> they still have the opportunity to protect themselves from unsigned code.
> At a Medium setting, prior to downloading and running executable software on
> your computer, Microsoft Internet Explorer presents you with a dialog either
> displaying the publisher's certificate, or informing you that an "unsigned
> control" can be run on your machine. At that point, in either case, you are
> in control and can decide how to proceed.

I appreciate your insightful opinion on this matter, however...

Even if you choose wisely, ActiveX is a hole waiting to be exploited and provides essentially no protection. As the folks at Microsoft know well, impediments are easily and commonly removed - and the use of the display box for popular applications is likely to result in the question being turned off in favor of easy access.

> As you know, Microsoft is committed to giving users a rich computing experience while providing appropriate safeguards. Most useful and productive applications need a wide range of system services, and would be seriously limited in functionality without access to these services. This means that many Java applications will have to go "outside the sandbox" to provide users with rich functionality. By signing code, a developer can take advantage of these rich services while giving users the authentication and integrity safeguards they need. Other firms such as Sun and Netscape are following our lead, and have announced that they will also provide code signing for Java applets. Microsoft will also be providing an enhanced Java security model in the future, giving users and developers flexible levels of functionality and security.

I appreciate your insightful opinion on this matter, however... "...while providing appropriate safeguards" is just not true. Microsoft has a long history of providing systems with no protection, and only recently introduced the first system with even mild protection in it's NT product. Java provides a lot of functionality within the "sandbox", but I am not an advocate of

Java either. The style of computing being pushed out to consumers

is inherently risky and must be implemented with substantial controls

if it is to be used safely. But this is not Microsoft's goal.

There is nothing wrong with having signatures, but it is no guarantee either.

> Microsoft takes the threat of malicious code very seriously. It is a

> problem that affects everyone in our industry. This issue is not tied to

> any specific vendor or group of people. All of us that use computers for

> work, education, or just plain fun need to be aware of potential risks and

> use the precautions that can insure we all get the most out of our

> computers. For this reason, we are committed to providing great safeguards

> against these types of threats in Internet Explorer. We expect hackers and

> virus writers to get increasingly sophisticated but we pledge we'll continue

> to keep you and us one step ahead of them.

I appreciate your insightful opinion on this matter, however... Microsoft

still has not addressed Work Macro viruses, PC viruses, Windows

viruses, etc. The claim that "Microsoft takes the threat of malicious code very seriously" is ludicrous on its face.

This is

the same company that has distributed viruses to its customers because

it didn't do adequate checking of its distributions for known viruses.

This is the company whose Windows installation deleted all of the

README files on a system when the user upgraded. This is the same

company that continues to ship software with inadequate

protection.

All of this "perception management" doesn't change the fact, and it shouldn't sway the readers of this letter either.

FC [Fred Cohen can be reached at tel:510-294-2087 fax:510-294-1225]

[NOTE: I usually truncate all but a salient excerpt from included message

text on which a responder is commenting. In this case, it would have

required too much editing effort to delete the interstitiated originals

and still convey the sense of the relevant references. Your cross-reading

effort would also have been much greater. PGN]

✉ Re: MS on the CCC ActiveX virus ([RISKS-18.83](#))

<Steve_Kilbane@cegelecproj.co.uk>

Fri, 21 Feb 1997 17:38:47 GMT

> Other firms such as Sun and Netscape are following our lead, and have
> announced that they will also provide code signing for Java applets.

This is what annoys me most about this response: not only are Microsoft attempting to justify giving away the family silver, but they're also trying to imply that they're the ones responsible for the idea of code signing (just like MS and IBM have been implying that they've recently invented multitasking....).

When Java was announced at the Sun UK User Group conference back

in '95,
Chuck McManis said that code signing was in the plan, and that
the main
problem was the US export controls. He also commented that while
exporting
decent authentication software wasn't allowed, Sun had been told
that there
was nothing wrong, in principle, in shipping "a library for
doing math with
really big numbers". :-)

I wasn't following Java back when it was called Oak and set-top
boxes were
the name of the game, but I wouldn't be hugely surprised to
discover that
signed code was part of the plan even then. Anyone with more
authority care
to comment?

steve

ActiveX - a real world view

"John Pettitt" <jpp@cybersource.com>
Fri, 21 Feb 1997 14:44:07 -0800

While at a technical level, most of what has been said about
ActiveX and
security is correct. It's worth noting that users take code from
untrusted
sources all the time. While the experience of users says that
code they
download is mostly well intended (even if it has harmful bugs)
it's going to
be a hard sell trying to convince them that a limited Java model
is "better"
than ActiveX.

I'm using ActiveX on software.net (a restartable download
control from

centric development). Our experience is that it has a close to 100% acceptance rate by users (as compared to less than 50% for Netscape plugins). Certainly the cute "certificate" dialog has a very positive impact on user confidence.

We're about to start signing all the downloads from software.net (we download 1600+ commercial titles). We had an interesting debate about the ethics of signing other people's code. However the user perception issue won out, we will sign the archives that we download (but not the applications inside them).

In all the research we've done (and we download a lot of software) users' biggest perceived risk is that their credit card # will be stolen. The idea that the copy of Microsoft Word we download to them may not be the real thing does not even feature.

John Pettitt, jpp@software.net, EVP, CyberSource Corporation,
408 260 6013

✶ ActiveX exploitation code in iX 3/97

Thomas Koenig <ig25@mvmmap66.ciw.uni-karlsruhe.de>
Fri, 21 Feb 1997 20:05:41 +0100 (MET)

iX Magazin 3/97 (a German computer magazine) has a fairly technical article by Lutz Donnerhacke and Steffen Peter about the ActiveX hack.

Parts of the article can be found at <http://www.heise.de/ix/artikel/1997/03/090/code.shtml> ; the exploitation code is available at <http://www.heise.de/ix/artikel/1997/03/090/code.shtml> (minus some delay loops).

Thomas Koenig, Thomas.Koenig@ciw.uni-karlsruhe.de

[iX = neun? nein! PGNeu'n]

✉ Re: Bank Sued for Racist E-Mail (Kennedy, [RISKS-18.83](#))

Jon Seymour <jon@zeta.org.au>
Sat, 22 Feb 1997 07:23:10 +1100

> :: Mail sent on Jan 28th. Suit claims little or no action was taken against
> those who spread the message, although the company acknowledged an incident
> did take place and it was "putting into effect disciplinary actions" against
> the perpetrators.
>
> DMK Comment: Another company is being sued for objectionable content of
> employee computer use.

The corporation is being sued, I think, because it allegedly tolerates a culture of racism. At least part of (perhaps all?) the evidence for this happens to be an e-mail passed between employees. How this e-mail came to the attention of those who wish to sue has not been specified - at least by this discussion.

There is a risk here if the courts were to find the corporation

liable

because it failed to prevent the e-mail being distributed in the first place

(hardly practical or, indeed, desirable) or it is found responsible for the

attitudes of its employees _soley_ on the basis of such e-mail.

The relationships that existed between the people with whom the e-mail was

communicated are surely relevant. For example, if the e-mail was sent to

all the white members of a group, but specifically not to the black

members of the same group by the supervisor of that group then I personally

think that might well be considered unprofessional behaviour in need of a

disciplinary response. If it was sent to the black members too then that

would either be stupid, tactless or both stupid and tactless.

If the e-mail was sent between friends then, yes, the ethics of the situation

are different, even if the ethics of the "humour" itself are not.

E-Mail should not, ipso facto, be eliminated as evidence simply because it is

e-mail. E-Mail happens to have the property, unlike the spoken word, of

automatically leaving traces of itself about the place. This means that,

technically, it is good evidence. Of course, one assumes that the e-mail in

question was not digitally signed and is therefore not _very_ good evidence

: -).

Of course, this is not to say that e-mail should always be used as

evidence. Clearly privacy concerns are important. If the e-mail in this case

came to light because a system administrator snooped it, then it probably

shouldn't qualify as evidence. If it came to light because one of its recipients decided to divulge it then it's fair game. What's the bet that it came to light because someone printed it and pinned it to wall?

It would be interesting to learn more about the circumstances of this matter and what the eventual outcome of the case is. One suspects that the media will not report it unless there is something controversial about the ruling.

jon seymour

✂ Re: Who made the call in the Moldova porn scam? (Claar, [RISKS-18.83](#))

John Kohl <jtk@atria.com>
21 Feb 1997 14:04:46 -0500

I'd expect that the consumers affected would have the option of suing for actual damages (i.e. phone charges) from the fraudulent scam operators. This would be akin to having your car stolen and illegally parked--the parking tickets would come to you as the registered owner of the vehicle. You could attempt to get the thief to cover your costs (if you can identify him/her :), or argue with the municipal parking clerk to waive them.

==John

✶ Re: Who made the call in the Moldova porn scam? (Claar, [RISKS-18.83](#))

Marc Horowitz <marc@cygnus.com>

21 Feb 1997 15:25:09 -0500

>> ... But if you steal my phone line, AT&T thinks I'm at fault.

This is an improper analogy. A more proper analogy: If someone steals your car, and crashes it into another car, totalling both, the owner of the other car is not responsible. If someone steals your phone line and makes lots of calls, AT&T is not responsible.

The difference is that in the car situation, one or both insurance companies will pick up the costs (in most states), and then try to recover from the thief. You probably don't have wire fraud insurance. But perhaps AT&T should.

In reality, such insurance would probably not be a good investment for either AT&T or the insurance company, because wire fraud, unlike car theft, is guaranteed to happen to AT&T. Instead, AT&T increases rates a little (in effect, implicitly selling you the wire fraud insurance) to cover the costs of fraud. This seems fair, because wire fraud is relatively unlikely for any particular customer, just like car theft.

Of course, as you point out, AT&T is better off if they can make you pay for it, but that doesn't mean AT&T is right, it just means they're acting in self-interest, which is exactly what most of their shareholders would want.

Marc



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 18: Issue 85

Tuesday 4 March 1997

Contents

- [Bremen hospital computer withdrawn](#)
[Debora Weber-Wulff](#)
 - [*Dallas Morning News* Web page on Timothy McVeigh](#)
[PGN](#)
 - [Password-Sharing Thwarts Web Revenues](#)
[Edupage](#)
 - [Tattooing SSNs on dogs to secure against dognapping?](#)
[Pat Sullivan](#)
 - [Worcester Poly student finds Internet Explorer flaw](#)
[PGN](#)
 - [Comments and corrections regarding Authenticode](#)
[Bob Atkinson](#)
 - [Not dead yet - I'm still 3 degrees!](#)
[Matthew M McNally](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ Bremen hospital computer withdrawn

Debora Weber-Wulff <weberwu@tfh-berlin.de>

28 Feb 1997 21:12:17 GMT

[I am translating a condensed version of an article that appeared in a German newspaper. I did not write the program!! That ActiveX translation caused a *lot* of wind! -dww]

>From the *Ostseezeitung*, 28 Feb 1997 [I was in Rostock, Germany at a wonderful conference]: German hospitals are using computer programs to calculate if it makes financial sense to keep patients in intensive care on the life support machines. This was published in the German weekly "Der Woche" in the most recent edition. According to "Der Woche", the computer assesses the vital statistic data kept on patients and computes the likelihood of the patient surviving. The health authorities in Bremen yesterday told the hospital "Links der Weser" to stop using this program, as it is unethical. The Marburger Bund, a doctor's association, warned the same day that such programs are being introduced into hospitals around the country. The chairman of the Marburger Bund, Frank Ulrich Montgomery stated: "When the survival of a person is dependent on money-based criteria, then we have ethically reached the situation where the Nazis left off." However, Montgomery notes that it is indeed useful to track data on patients in the intensive care units, as there are quite a number [he said "infinite", but I don't believe that! -dww] of information points collected about patients. The City Hospital Merheim in Cologne will continue to use the program. The head of the surgery department, Prof. Hans Troidl, called

the press reports "stupid and irresponsible." The program determines the condition of a patient determined by the blood values and the body temperature and such. In addition, the program notes how many patients with the same values survived. [more quotes and stuff deleted] The decision how to help the patient is solely the responsibility of the doctor and cannot be delegated to a computer. The computer is only a consulting aid. [A doctor in Bremen] said that we should be considering the costs of treatments, however, and begin discussions on this topic. [more quotes, nothing new.]

Coming down the steps at my train station at home I saw the evening yellow press has the "Dr. Death Computer" in big headlines, so stay tuned for a big row in Germany about such programs. The risk? Don't write programs without weighing the effect it might have on public sensitivities! (Check out the ACM Code of Ethics!)

Debora Weber-Wulff, Technische Fachhochschule Berlin, FB Informatik,
Luxemburger Str. 10, 13353 Berlin, Germany weberwu@tfh-berlin.de

***Dallas Morning News* Web page on Timothy McVeigh**

"Peter G. Neumann" <neumann@csl.sri.com>
Tue, 4 Mar 97 08:03:26 PST

The *Dallas Morning News* posted an item on its Web page on 28 Feb 1997 (although the newspaper story did not appear until the following day), alleging the existence of a report stating that Timothy McVeigh

had admitted
to his attorney Stephen Jones that he (McVeigh) was responsible
for the
Oklahoma City bombing that killed 168 people at the Alfred P.
Murrah Federal
Building in April 1995. Jones at first denied the existence of
the report,
but now admits the report does exist -- although he denied its
representing
a confession. What makes the case RISKS-relevant is that Jones
is charging
that the *News* stole the document in January as a result of a
computer
break-in that enabled access to confidential defense materials.
[Source: a
Los Angeles Times item, 4 Mar 1997, itself including AP
sources; seen in
San Francisco Chronicle of that date, A2.]

✶ Password-Sharing Thwarts Web Revenues (Edupage)

<educom@elanor.oit.unc.edu>

Sun, 23 Feb 1997 12:05:05 -0500

Web entrepreneurs who charge subscription fees for accessing
their Web sites
are finding their customers are passing along their passwords to
friends,
relatives, etc., thus diminishing Web operators' potential for
making their
venture pay off. "Everybody on the Internet who sell
subscriptions has this
problem to one degree or another," says a producer for
SportsZone. A
technical fix is possible, but Web site operators are reluctant
to make
things more difficult for legitimate subscribers to log on.
Meanwhile,
Internet Billing offers software that allows Web sites to limit

how many
times the same password may be used each day -- a solution that
would
probably keep some of the piracy down, but runs the risk of
alienating
paying customers who just want to log on a lot. (*Wall Street
Journal,* 21
Feb 1997; Edupage, 23 February 1997)

🔥 Tattooing SSNs on dogs to secure against dognapping?

Pat Sullivan <Psullivn@aol.com>
Sun, 2 Mar 1997 17:35:07 -0500 (EST)

[On WJFK-FM, an advocate of Forepaws (an animal rescue group)
recommended
tattooing your SSN on your dogs to combat dognapping, and
suggested that
this has become a semistandard practice.] This is an
astoundingly poor
idea, considering the well-known sensitivity of the SSN -- which
should
never be used to ID something for which the likelihood of theft
is high
enough to warrant a confidential ID. It exposes the SSN to
exactly the
worst people to have access to it. This is a case where the
cure is worse
than the disease. Also, it could actually stimulate dognapping
since it
adds information value to the dog. [Pat's letter to the station
deleted.
PGN]

Pat Sullivan

[Certainly gives you cause for pause (four paws?) that RISKS
is emBARKing
on animal-related risks of SSNs. How about BARKcoding? Also
intriguing

is that Pat lives on Barker Hill Road, perhaps doggedly. PGN]

⚡ Worcester Poly student finds Internet Explorer flaw

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

Tue, 4 Mar 97 08:03:26 PST

Paul Greene, a student at Worcester Polytechnic Institute, yesterday posted a note about a flaw discovered by him and colleagues, which allows Web servers to execute arbitrary commands on users of Microsoft's Internet Explorer 3.01 browsers (and possibly earlier versions?). The flaw can be triggered **without** using ActiveX, and even if IE is set to its highest security level. Windows 95 does not prompt you before merrily executing. A .URL file attack works on both Windows 95 and NT 4.0. Greene's site is <http://www.cybersnot.com> and MS's impending fix is posted at <http://www.microsoft.com/ie/default.asp> . [Source: AP item, seen in **San Francisco Chronicle**, 4 Mar 1997, C4]

⚡ Comments and corrections regarding Authenticode

"Bob Atkinson (Exchange)" <bobatk@EXCHANGE.MICROSOFT.com>

Mon, 3 Mar 1997 19:23:15 -0800

As the architect and primary implementor of the Authenticode code-signing technology (boy, that'll get me mail :-)) found in Internet Explorer 3 and in Windows NT 4, I think my perhaps somewhat lengthy and clearly

very biased
perspective on some recent articles might be of interest to
others.

Bob Atkinson

> From: "Theodore Y. Ts'o" <tytso@MIT.EDU>
> Subject: Re: Myths about digital signatures (Felten, [RISKS-
18.83](#))

>
> For example, if an Active X component has a loophole where
(with the right
> document) said component can be induced to interpret and
execute arbitrary
> Visual Basic statements, even if the signer was honest, and
legitimate, and
> properly went through all of the Microsoft certification
procedures, it
> still might be possible to exploit a security bug in the
Active X component.

First, a correction. Microsoft does not have any 'certification
procedures'
with respect to the integrity or lack thereof of third party
applications
against security attacks. There is no magic bullet that would
enable us to
make such statements. Software developers, as they always have
been, have
the responsibility of themselves exercising appropriate diligence
in this
regard.

We do, however, offer system services that aid developers in this
endeavor. For example, the underlying Authenticode engine is
available for
use by applications so that, say, if they themselves are an
execution engine
which might from time to time download possibly malicious code,
they can
apply the same gatekeeping checks as the system's download engine
applies. This was, exactly, intended to address the scenario
describe here
(see the "WinVerifyTrust API" if anyone is interested).

As another example, the overall system infrastructure, which includes the Java VM and its attendant sandbox, has mechanisms for classifying ActiveX components as "safe for scripting" and "unsafe for scripting;" a similar mechanism applies to "safe for initialization" (from data on web pages). These are designations assigned by the ActiveX component developers themselves. In short, components that designate themselves as 'safe for X' can be interacted with by (possibly malicious) code inside the sandbox; code designated as 'unsafe for X' is prevented by the system from being instantiated or interacted with by sandbox code. The point being that the system provides the component developer flexibility in balancing his development time and effort with the amount of richness available to his component once downloaded.

> The Java security model at least *thinks* about this issue, where as the
> Active X approach completely punts about this concern.

Having spent considerable brain cycles on the issue over the last couple of years, you'll I hope pardon me if my opinion differs from the thought expressed here.

Users want and demand a rich computing experience. Users want software that does interesting, important, and useful things for them, be that Navigator plug-ins, arbitrary EXEs, .Zip files, Java (system) classes, ActiveX controls, or something else. The same security issues being discussed with respect to ActiveX apply equally to all these other forms of

application,
all of which in the course of doing interesting and useful
things on behalf
of the user is going to at times need to be given access to
information or
capabilities that could be used for evil instead of goodness.

With traditional software distribution channels (Egghead,
Computer City,
...) you know where the code came from because it says so on the
box, and
you trust the retailer to sell you only legitimate product that
hasn't been
tampered with. Got a problem with the program? The guy on the
box is who you
call; he sure doesn't want the embarrassment or liability of
shipping
product that ends up having a virus in it, so he takes care not
to do
so. The combination of criminal and tort laws together with a
company's
desire to stay in business and enhance its reputation works
together to
create a system that supplies customers with rich, useful
software at a
minimum of risk.

We have decades if not centuries of experience with this model
of conduct
between supplier and customer. It seems to work pretty darn well.

In the online world, users have heretofore installed software
manually, by
way of manual download. In doing so, they have had to resort to
ad-hoc and
often naive mechanisms for judging the risk they are taking in
doing
so. "Just where did this code come from? Who is responsible for
what it
does? And has it been tampered with? How do I know?" The online
distribution
channel has lacked mechanisms that provide the accountability
present in

traditional channels.

We can make users lives dramatically better by automating the online software installation process. The rich, useful code can just always be simply there right when you need it, rather than your having to understand what code it is you're missing, hunting around to find it, and having to have the computer experience to figure out how to manually install it.

In addition, we can provide mechanisms that bring to bear in the online world the same forces successfully used to manage risk in traditional channels, mechanisms that can help users be conscious of the risks involved and make informed choices about them. These mechanisms are particularly important to have in place when installation is automated, as it is in IE3, but the mechanisms are also valuable and useful even when installation is done manually.

> From: fc@ca.sandia.gov (Fred Cohen)

> Subject: Re: MS on the CCC ActiveX virus ([RISKS-18.83](#))

> I appreciate your [BradSi's] insightful opinion on this matter, however...

> Anyone can get a signature key without authenticating their legitimacy.

> It's relatively easy to break into a system and take a legitimate key.

It is true that the user's understanding and the care with which he manages his private key is an important part of an overall security infrastructure. Flaws in any one part of that overall infrastructure may compromise the system as a whole. However, compromise of private

keys is a concern that IMHO warrants less worry than other aspects of a system might.

In Authenticode as implemented in IE3 and NT4, the private keys are managed by the system's cryptographic provider infrastructure (CryptoAPI), which enables a number of different cryptographic devices to be used transparently by applications. Several different cryptographic hardware devices are on the market that support CryptoAPI, offering extraordinarily good, virtually foolproof private key protection in a range of prices from a couple of hundred to a few thousand dollars (see, for example, http://www.spyrus.com/whats_new/pr_csp.htm, or <http://www.bbn.com/offerings/sksign.html>).

Such hardware devices and the increased key protection they provide are likely to be well worth the investment, especially for commercial enterprises in the business of software publishing. Indeed, from my own personal perspective it can be argued (disclaimer: I am not now, nor ever have been a member of the legal profession) that given the modest costs and given the nature of being in the software business to not take such precautions might be considered negligent on the part of such an enterprise.

For those curious: at the present time, the private keys with which Microsoft signs code that it publishes are managed inside BBN SafeKeyper boxes housed in a guarded steel and concrete bunker. Even were a SafeKeyper to somehow be physically stolen, these cool little boxes have several

elaborate internal defenses designed to have the box destroy itself rather than compromise its keys. As I understand things, a military variation on the SafeKeyper technology is used as an integral part of launch control of nuclear missiles on submarines in the US Navy.

In the absence of a hardware device, CryptoAPI provides an in-the-box a software-implementation of the cryptography; however, when this cryptographic provider is used with Authenticode, the private key is not in fact kept online, but rather on a floppy disk, which need be inserted only during the actual act of code signing, hopefully on a managed, virus-free 'release environment' machine used to protect against this and a whole host of other more traditional potential virus attacks.

> The default may be changed by the user for one use and remain changed.
> Other flaws in Explorer may be used to turn that feature on - then look out.
> > The CCC demonstrated its malicious executable code running on Microsoft
> > Internet Explorer 3.0

This is true, as the demonstration was made, but it is misleading, as it leaves out significant contextual information. The CCC demonstrated code which, if it had been actually deployed, would, as I understand things from the press descriptions I have seen, carry out actions which are out-and-out-theft. Theft is illegal. You can go to jail for it, if they catch and convict you.

Let's look at that for a moment. There are the following ways in which that

malicious code could get on a user's machine:

1. The user can choose to bypass the security support provided by the system by setting his security level to 'none' or 'medium'. The CCC control was unsigned, and thus cannot be installed by IE unless the user overrides the protection provided by the system.
2. The code could be signed, and then downloaded by IE3, and accepted by the user. That is, the crooks can if they like leave their clear, unsmudged fingerprints all over their illegal device. This makes catching and convicting the responsible party somewhat easier.
3. Some well-intentioned software agent other than IE3 can download and install the malicious code. Such agents, would, however, have the same responsibility for exercising due diligence in protecting the user as IE3 itself has. Fortunately (see above), the mechanisms are available in the system infrastructure to allow them to do this.

In the absence of the user bypassing the system's security infrastructure, which as was mentioned is highly discouraged, then should the system be attacked by a malicious ActiveX control, some piece of malicious or negligent digitally-signed code that was downloaded is ultimately responsible for carrying out the attack or allowing it to occur.

The mechanism which prevents this from happening is the deterrent of a reasonable expectation of getting caught and being held accountable for one's actions. This is the same mechanism used to great effect in the rest

of a free society to balance freedom of action and unencumbrance by red tape with society's need for safety and protection.

The presence of digital signatures on code does not remove the need for law enforcement agencies to do their investigative work when confronted with a crime; their detective and analysis skills will continue to be valuable and needed. Even in the absence of an audit log of execution (a very good idea, where technically feasible), if you eat hamburgers at Restaurant X, and you get sick, and Fred eats hamburgers at Restaurant X, and he gets sick, and so on, chances are that there's something wrong with the hamburgers at Restaurant X. Or if you drink fruit juice from Company Y ... you get the idea. Effective and successful criminal prosecutions are regularly and routinely made on less than perfect evidence, often much less clear than we're discussing here.

What digital signatures on code provides is a robust and unforgeable attribution of responsibility for publication once the actual offending code is identified. And, as implemented contractually and technically in the present release of Authenticode, when you sign code you are most certainly taking explicit responsibility as the code's publisher, an action not to be taken lightly from a legal point of view. The additional ability to have third parties digitally "endorse" or "rate" works published by others we have always thought to be a very useful and valuable concept, but it is a separate and distinct one from that of signing as the publisher.

> As the folks at Microsoft know well, impediments are easily and commonly removed - and the use of the display box for popular applications is likely to result in the question being turned off in favor of easy access.

Yes, the concern that inconvenience or annoyance causes the end-user to bypass the security infrastructure (see #1 above) is an important consideration. However, I am optimistic given our experience to date that we've done well in this regard, though only time will tell for certain. Educating users not to lower their security level is extremely important; we're working very hard on educational initiatives like the Security Advisor program (<http://www.microsoft.com/security>).

Moreover, in the Authenticode infrastructure is the notion that one can come to 'trust' certain publishers. Code that is legitimately signed by a software publisher who is listed by the user as trusted is automatically approved for installation without user intervention. For example, if Microsoft Corporation were listed, then code signed as being published by Microsoft will be downloaded and installed without any dialog box or other repeatedly-annoying UI. The net effect is a mechanism that allows the user to bypass redundant and repeated prompts for the same approval _without_ compromising his protection in any way.

Within intranets, even greater protection can be achieved by enforcing download and signature-checking policy within a company's firewall. This can be done, for example, with TIS's Gauntlet Internet Firewall

(<http://www.tis.com/docs/corporate/press/96/mspr.html>).

> From: Steve_Kilbane@cegelecproj.co.uk
> Subject: Re: MS on the CCC ActiveX virus ([RISKS-18.83](#))
>
> > [MS Press Release:] Other firms such as Sun and Netscape are
> > following our lead, and have
> > announced that they will also provide code signing for Java
> applets.
> not only are Microsoft
> attempting to justify giving away the family silver, but
> they're also trying
> to imply that they're the ones responsible for the idea of
> code signing
> [...]
> I wasn't following Java back when it was called Oak and set-
> top boxes were
> the name of the game, but I wouldn't be hugely surprised to
> discover that
> signed code was part of the plan even then. Anyone with more
> authority care
> to comment?

I think too much is being read here into our press release.

Invention of basic ideas and usable, successful, practical wide-
spread
deployment of implementations of ideas are different beasts.
Both are
important, and both are needed. Both require some amount of
creativity and
innovation.

The general notion of digital signatures has been around for
quite a
while. Just to take one example implementation from many
possibilities,
Apple some time ago shipped in their OS a "digital signature on
documents"
infrastructure (whose name alas escapes me at the moment). The
relevant
technical standards used in Authenticode (X.509 and PKCS #7) are
also not

new by any stretch of the imagination. With respect to signed
code,
various Java-related web pages on the Sun web site circa early
summer 1995
indeed did mention in passing that it was an interesting idea to
apply
digital signatures to code. Clearly Sun was at that time
exploring this
interesting idea. However, no insights were offered as to the
actual
policies or architecture that might be involved. To be just a
little
overly-severe, what I recall was little more than simply "digital
signatures" and "downloaded code" being mentioned in the same
sentence.

IMHO, the most important innovations of Authenticode on prior
general
practice in the industry lie in the area of usability,
especially as related
to the user's understanding of and administration of trust. You
might
notice, for example, that the certificate dialog simply states
"X is
published by Y under credentials issued by Z," as in "Surround
Video Control
is published by Microsoft under credentials issued by Verisign"
a simple
"brand of identity" approach rather than the historical approach
of
thrusting upon the user a whole chain of delegated
identifications. Also,
appropriate clickable hyperlinks are provided on the prompting
dialog,
allowing both the publisher to set appropriate expectations with
the user as
to what his code is going to do, and for the credentials agency
to inform
the user of its identification policies, all before the user has
make the
decision of whether to allow any of the publisher's code to run
or
not. Third, as was mentioned, repeated prompts for essentially

the same approval can be easily and simply automated without loss of security. Fourth, the fact that we focused on mechanisms whereby signatures can be physically inserted within existing file formats (.EXEs, .CAB, .class, etc) rather than as separate files increases usability by avoiding the need to keep multiple files in synchronization.

None of these ideas is by itself especially deep. But taken together, I submit that the overall user experience is significantly more straightforward.

Finally, there is the simple fact that despite the (welcome!) future plans in the area of code signing expressed by both Sun and Netscape, Authenticode is still the only actually-deployed code signing infrastructure. It's seven months into widespread shipment, nine or ten months since it's first beta, close to a year since its first public demonstration, and close to fifteen months since it's announcement. Ideas are important, but it's difficult to impact users unless you actually ship product.

⚡ Not dead yet - I'm still 3 degrees!

Matthew M McNally <mm3d+@andrew.cmu.edu>

Mon, 3 Mar 1997 09:13:45 -0500

Suffering from a sinus infection, I went to my doctor's office in search of answers. A standard operating procedure in the US is for a nurse to take a patient's temperature, blood pressure, and to ask a few questions before the

doctor comes in to spend some time with the patient.

Well, they have these new "ear" based thermometers (I won't even hazard a guess as to how they really work) which they place in your ear and "push a button" to read the patient's temperature - at which point the patient feels/hears a small click in their ear and a number appears on a small LCD display on the device.

My first reading came up "3" - my second reading came up "3" at which point the nurse shook the device - my third reading came up "3" - at which point I asked the nurse what the "3" really meant.

She replied, "3's an error code."

"Hmmm, any idea what it means? Am I broken?"

"Nah [laughs], it just means something isn't right, this happens a lot in the mornings before it warms up but not usually in the afternoon...I don't know what it means."

At this point she opens the door and yells across the office for another nurse to come in - who does, takes the 'earometer' if you will, places it in my ear and "click" I'm now 94.7! Hurray they have *a* number!

The first nurse writes 94.7 down, and moves on to the more traditional method of taking my blood pressure...

The Risks? A medical device with unusable error codes (as suggested by my user study N=1) and an inherent belief that whenever the system appears to work, that it is actually working. Let's hope people working

with infusion pumps, heart monitors etc. etc. are a little less trusting in this master we call technology.

Matt McNally

PS - This probably wouldn't have drawn my attention if I hadn't literally had 15 minutes to ponder the event while the local druggist's cashier attempted to "manually" enter my credit card number for a purchase approval. It seems this national chain no longer trains their cashiers to handle credit card approvals outside of the built-in register function. The store basically came to a halt until the druggist (reading instructions from a card) was able to call his merchant account's approval system directly.



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 18: Issue 86

Wednesday 5 March 1997

Contents

- [ActiveX security? TISK, TISK](#)
[Brent Laminack](#)
- [Re: Comments and corrections on Authenticode](#)
[Li Gong](#)
[Jerry Leichter](#)
[David Hopwood](#)
[A. Padgett Peterson](#)
[Fergus Henderson](#)
[Glenn Chambers](#)
[Steve Kilbane](#)
[Kevin McCurley](#)
- [Info on RISKS \(comp.risks\)](#)

⚡ ActiveX security? TISK, TISK

Brent Laminack <brent@cc.gatech.edu>
4 Mar 1997 22:03:15 -0500

The recent comments about ActiveX and Authenticode have been useful and

constructive, but have focused so far on how *an* ActiveX control operates.

We have yet to cross into that shadowy world that RISKS readers are all to

familiar with. The realm of what I call TISK: Timings, Interactions and

Side-effect Kollisions (sic), as in the support people saying "TISK, TISK

Joe User has a problem that we can't duplicate here..."

Consider two ActiveX controls. One provides a control similar to the Win95

"Start" button with all the commands on the user's computer presented in a

list to choose from. Suppose it keeps these command names in a preferences

file such as C:\windows\mycommands. The file may contain a list such as:

Word, Excel, format c:, IE3, etc.

Consider a second ActiveX control that provides a "cron" facility. This

automatically wakes up at a specified time and executes a list of commands

for housekeeping such as backup, defrag, etc. Suppose it keeps its list of

commands in, say, for instance C:\windows\mycommands. You see it coming,

right? The second control finds the file written by the first one and

dutifully fires up Word, Excel, and then formats the C drive. Commands after

this one are of diminishing consequence.

OK, you're stuck. Your hard disk is wiped. Where are the fingerprints for

Authenticode? Even if you do get them, who are you going to sic the law

enforcement people on? Both controls did exactly what they were designed to

do, exactly what they advertised to do. Who are you going to sue? Obviously

neither "misbehaved." What did in your disk was an unforeseen

interaction
between the two. TISK, TISK. I imagine that with a bit of
thought work it
would be possible to come up with a co-operating gang of ActiveX
controls to
do deliberate theft via collusion where each program is only
doing what it's
"supposed" to, yet the total of their activity is much greater
than the sum
of the parts. Yes, non-linearity is clearly at work here in the
interaction
of the components. The only way to avoid this would be to
strictly decouple
them, by not allowing any to share information with the other,
such as
giving each its own private file-space to write in. This, alas
is not the
case.

Brent Laminack (brent@ecweb.com)

✶ Re: Comments and corrections on Authenticode (Atkinson, [RISKS-18.85](#))

Li Gong <gong@games.Eng.Sun.COM>
Tue, 4 Mar 1997 23:01:47 -0800

I certainly will not be the only person to feel the need to
respond to Bob
Atkinson's article in [RISKS-18.85](#). I emphasize that this is a
technical,
not political, response. Basically, 2 comments and 1 challenge
to Bob and
Microsoft.

> And, as implemented contractually and technically in the
present
> release of Authenticode, when you sign code you are most
certainly

> taking explicit responsibility as the code's publisher, an
action
> not to be taken lightly from a legal point of view.

Saying code signing gives you accountability is too simplistic.
First, you might not have an audit trail to use as supporting
evidence. Second, history says that if a piece of software
needs to
carry serious, legally binding liability, there would not be a
Microsoft or a software industry in general. Thus
accountability is a
potential, not a reality.

> ... Authenticode is still the only actually-deployed code
signing ...

Netscape Navigator 4.0beta has code signing (originally shipped
1996),
and JavaSoft's JDK1.1 has applet signing (alpha last Nov and
final
version shipped Feb 97). (Potential bugs is a different
discussion.)

Now the challenge. Java has the potential to give you fine-
grained access
control, whether the code is signed or not. To realize this
potential
today, one might have to customize the SecurityManager. Future
versions of
JDK will make such functionality easier to use.

ActiveX/Authenticode, however, does not seem to have such a
potential. So
tell me how to configure a Win95 system such that an ActiveX
control (or
component or whatever) can read/write only to directory /tmp (or
C:\tmp)
while it is prevented from all other file I/O?

Li Gong, Java Security Architect, JavaSoft

✶ Re: Comments and corrections on Authenticode (Atkinson, [RISKS-18.85](#))

Jerry Leichter <leichter@lrw.com>

Tue, 4 Mar 97 23:18:55 EDT

Bob Atkinson argues that digital signatures on downloaded code, at the least, allow you to identify someone who sent you "bad code" for legal action.

There is so much wrong with this claim that it's hard to imagine anyone would make it. To mention just two things:

1. The "evidence" - the digital signature - that would presumably be used against the attacker is stored ... on the very machine that is being attacked. On a system like Windows 95, which provides absolutely no internal protection, that evidence will last for a few milliseconds. (Admittedly, a protected system like NT *could* write secure logs of signatures that had been recently accepted. However, it'll be quite some time - if it ever happens - before the existing base of unprotected systems is replaced by protected ones.)

2. Mr. Atkinson makes the assumption that the malicious code can be identified. Sure, if it immediately does something that you can see, things are easy. But if it does something indirect; or waits until executed the 100th time; or modifies some *other* program so that *it* later does something nasty;

then tracking the down the source of the original corruption

will be extremely difficult. Hell, tracking down "memory poisoning" *bugs* is extremely difficult - and these are random events that make no direct attempt to cover their tracks.

The traditional boxed software set from a local store is safe for many reasons - but some of the important ones related to the inherent limitations of the traditional distribution medium. It's fairly difficult and expensive to put together the boxes, documented, printed CD's, and such. Distributing them to stores adds much more expense - and at each step of the way, there are people to talk to, papers to sign, money to change hands, records to be made. The advantage of on-line distribution is that it cuts away all these layers and delays and costs. But in doing so, it also makes attacks much cheaper, easier, and more anonymous. A signed piece of code shares one characteristic with software in a box: A mark that can, with reasonable though varying confidence, be ascribed to the person who created the boxed set/signed software object. But the two are different in so many other fundamental ways that to attempt to argue the acceptability of one on the basis of experience with the other is simple sophistry.

"People want nifty things on their machines; they don't want security mechanisms getting in the way." People haven't yet been badly burned. Look how many years it took to get even rudimentary safety devices into cars.

Jerry

✶ Re: Comments and corrections on Authenticode (Atkinson, [RISKS-18.85](#))

David Hopwood <hopwood@zetnet.co.uk>

Tue, 4 Mar 1997 04:49:45 GMT

I interpreted Theodore Ts'o as meaning checks on the signer, not the signed code - but in any case, the fact that there is no means of auditing and certifying the security of controls can only worsen the situation, not improve it.

>Software developers, as they always have been, ...

By saying "as they always have been", you seem to be suggesting that this kind of security attack is a serious concern for all applications. That is far from true; it normally only applies (with varying seriousness) to network servers and clients, `suid/sgid` programs, helper apps, plug-ins, and other programs that are passed data from a source which is less trusted than the program itself. If all programs were passed data from untrusted sources, computer security in general would be in much more of a mess than it is currently in.

In cases where a program acts on untrusted data, it isn't valid to make a judgement of its security simply on the basis of trusting that the writer of the program is not malicious. You also have to consider how competent they

are at writing secure code.

Users of ActiveX are being encouraged (by Microsoft's documentation - I can provide examples if needed) to accept or reject controls based on whether they think the signer is malicious, not the stronger, and more relevant criterion of the author's competence. If they were to actually make realistic security decisions based on that stricter criterion, they should IMHO not be running any code whose URL and version number is specified by a web page that they have no reason to trust, as is typically the case when an ActiveX control is downloaded.

```
>... the overall system infrastructure ... has mechanisms for
classifying
>ActiveX components as "safe for scripting" and "unsafe for
scripting;" ...
>"safe for initialization" ...
```

These mechanisms are not sufficient; in practice, it isn't reasonable to expect developers never to create controls with exploitable bugs. Writing code that must be secure against data-driven attacks is hard, especially in languages such as C and C++ that have unchecked pointers and array accesses. If that were not the case, why are buffer overflow and similar attacks against suid Unix programs so common?

In Unix, normally only suid/sgid programs, and server daemons, are worth attacking in this way. Now, all signed ActiveX controls are worth attacking. If you can exploit a control to run arbitrary code, you can ensure that users will see someone else's signature when running your code,

which is something that you would only normally be able to do by forging that signature. The user cannot trace the malicious code to its author; instead the trace will end at the unfortunate person or company whose control was exploitable.

The situation is arguably worse than for conventional data-driven attacks, because it's effectively impossible to revoke a signed ActiveX control, if the attacker retains a copy of it. The most you can do is release a control with the same CLSID and a higher version number, and make sure that everyone who could be attacked has a copy of the new version in their control cache (the %windir%\occache directory). But that means everyone who uses ActiveX!

Anyone who does not have the updated version in their cache will simply download the copy of the old, exploitable version that was retained by the attacker. (Actually, there is also an implementation bug in the versioning mechanism in IE 3.0x, which means that the cache contents don't matter; an attacker can always cause an old version of a control to be downloaded).

The basic problem is that the architecture of ActiveX effectively makes all code used in controls security-critical. It must be assumed that there exist signed controls that can be used to run arbitrary code. I've seen several controls that crash IE if-and-only-if they are given long parameter strings (unfortunately for me, the resulting processor exception seems to be caught

without generating an error log or stack trace, which is likely to make exploiting this a tedious, but not impossible, process). I've also found a control which can be exploited in a different way to run arbitrary commands, but I'm still discussing the situation with the control's signer.

I do, however, intend to release that exploit publically, because I think it is the only way to demonstrate clearly the significance of data-driven attacks against ActiveX. Microsoft's response so far to concerns about ActiveX security has been one of denial and spin-doctoring; that has certainly influenced my decision to make the exploit public (that, and the fact that this particular exploit is trivial to implement once you know which control is involved).

>[...]

I entirely reject the claim that ActiveX provides the same level of accountability as is provided by traditional shrink-wrapped software distribution. In the shrink-wrap model, you trust the shop that is selling you the software. There is also no opportunity for untrusted data to be passed to the application when it is installed. With ActiveX, you have no basis on which to trust the web site which points to the control, because that site is not authenticated. Untrusted data can be passed to the control by its parameters (or using scripts, if `_in` in the signer's `opinion_`, it is safe for scripting).

Given these differences, the shrink-wrap analogy is simply

invalid.

In principle I think that digital signatures and/or secure channels can be used to provide a reasonable degree of accountability, but Authenticode is not, IMO, a good example of how systems using digital signatures should be designed.

>[...]

>In the absence of the user bypassing the system's security infrastructure,
>which as was mentioned is highly discouraged, then should the system be
>attacked by a malicious ActiveX control, some piece of malicious or
>negligent digitally-signed code that was downloaded is ultimately
>responsible for carrying out the attack or allowing it to occur.

Note that this argument does not distinguish between "malicious" and "negligent" code, either here or later in the article.

>The presence of digital signatures on code does not remove the need for law
>enforcement agencies to do their investigative work when confronted with a
>crime [...]

Let's be clear about this; an audit log is not feasible for ActiveX controls, because it could easily be overwritten or forged once a control is running. It is feasible for technologies that attempt to run code in a restricted environment.

>[...] once the actual offending code is identified.

Again, note that "offending code" here can mean the "negligent" code that

allows an attack to be launched by some other party.

>And, as implemented contractually and technically in the
>present release of Authenticode, when you sign code you are
most certainly
>taking explicit responsibility as the code's publisher, an
action not to be
>taken lightly from a legal point of view.

So if your code has an exploitable bug, you are taking legal
responsibility
for any damage done as a result of that? I think not; not only
is there no
legal precedent for this as far as I know, I suspect most
software publishers
would have to think very hard about whether they should continue
to sign code
under that agreement, if they can be held responsible for
anything that the
code does.

If there is not, in fact, any legal responsibility for writing
exploitable
code, and strong reasons to believe that a substantial minority
of controls
will be exploitable, the rest of your argument stands on very
shaky ground.

David Hopwood david.hopwood@lmh.ox.ac.uk, hopwood@zetnet.co.uk

[Re: Comments and corrections on Authenticode \(Atkinson, RISKS-18.85\)](#)

"A. Padgett Peterson" <PADGETT@hobbes.orl.mmc.com>
Tue, 4 Mar 1997 17:47:40 -0500 (EST)

Pardon me if I tend to read this with the same sort of
skepticism as Brad
Silverberg's pronouncement that all web browsers have the same

vulnerabilities.

Coming from the same company that gave us WORD macro viruses by the simple expedient of granting control to the opened document and making it impossible for the user to turn macros off *even if they want to*, why should we expect anything different here? An .EXE must be executed. ZIP files must be unzipped. Java must be enabled. In each case the user has a choice and can place a scanner/checker/validator/debugger between the download and the execution if desired.

Thus far, every request to "just say no" to MS has been rebuffed (WORD 7.0a and Office 97 do have a "warning" that is simple to turn off but no way to simply disallow macros altogether).

I do not disagree that sometimes I am willing to "trust" certain parties for download but that is primarily because I have initiated the contact and have been able to examine the download prior to allowing it to execute.

Could be in the minority, but do not want anything to happen on my machine that I have not given explicit approval for or requested. Is one thing to push a button and say OK, another to have something occur without my knowledge.

For one thing, my machines often are operating on the ragged edge. For another, what you request may not be feasible. Have experienced to much software that I knew I was installing (and had backed up relevant areas

first) blow up on me to grant *any* global permissions. What works with W95 may not work so well with Novell DOS 7.0.

My *choice* is to limit the functionality of my PC to those things which I allow it to do. Thusfar MicroSoft's intention in those programs I have purchased seems to be increasingly to take that choice away from me. There does not seem to be anything in your words which would change my mind.

Padgett

[Re: Comments and corrections on Authenticode \(Atkinson, RISKS-18.85\)](#)

Fergus Henderson <fjh@mundook.cs.mu.OZ.AU>
5 Mar 1997 14:00:45 GMT

>First, a correction. Microsoft does not have any 'certification procedures' >with respect to the integrity or lack thereof of third party applications >against security attacks.

That is precisely Theodore Y. Ts'o's point: Microsoft does not have any certification procedures that could prevent such attacks. As a result, there are significant risks associated with the use of Microsoft's Active X technology.

>Software developers, as they always have been, have the responsibility of >themselves exercising appropriate diligence in this regard.

True, but because third parties can provide potentially hostile input to Active X controls -- at least for those classified as "safe for initialization" -- the "appropriate diligence" for such an active X control is much greater than that required for an ordinary application. The "appropriate diligence" required is similar to the diligence required for a Unix setuid executable. And past experience suggests that this high level of diligence is often lacking: setuid programs are very often the cause of security holes.

>Users want and demand a rich computing experience.

Yes, but users also "want and demand" to be able to log into systems without having to type in any silly passwords... it is our job as computer professionals to educate users about the risks involved and wherever possible to protect them from such risks.

>We have decades if not centuries of experience with this model of conduct >between supplier and customer. It seems to work pretty darn well.

Yes. One of the reasons it works so well is that there is a reasonably hefty financial hurdle that you need to overcome in order to distribute software using traditional distribution channels. However the Internet promises to change that. The Internet is a very low entry-cost distribution mechanism, and while that is a very desirable property, it is not without its associated risks. Lowering the entry cost increases the chance of abuse. Furthermore, automating the process increases the chance

that abuse
may go unnoticed. So even if Active X were to faithfully imitate
traditional distribution channels in every other way, the risk
may well be
much higher. That is why I think we need to move to
technologies that offer
better security than either Active X or traditional distribution
channels.
Java applets are one such technology.

>2. The code could be signed, and then downloaded by IE3, and
accepted by the
>user. That is, the crooks can if they like leave their clear,
unsmudged
>fingerprints all over their illegal device. This makes catching
and
>convicting the responsible party somewhat easier.

A thief would of course be foolish to leave their own
fingerprints on an
illegal device. It would be much more sensible for them to sign
with a
stolen key. Now of course it may well be difficult for thieves
to steal
Microsoft's key, but all it takes is one careless vendor who
doesn't guard
their key well...

Fergus Henderson <fjh@cs.mu.oz.au> WWW: <<http://www.cs.mu.oz.au/~fjh>>

✉ Re: Comments and corrections on Authenticode (Atkinson, [RISKS-18.85](#))

Glenn Chambers <gchamber@mail.bright.net>
Tue, 4 Mar 1997 20:38:56 -0500 (EST)

I can't resist pointing out that Microsoft has suffered from
several highly

publicized incidents where they have shipped virus-laden MS Word (TM) documents on CD-ROMs, or placed them on their public web pages, etc.

Because (as nearly as I can tell from outside) it is entirely possible to 'sign' an *already infected* ActiveX component, it's only a matter of time before virus infected web pages make their debut.

Until and unless an 'Active-X sandbox' of strength equal to Java's is imposed, I'm sticking to non-Wintel hardware and software, and being very leery of what software I let execute on my machine.

Glenn Chambers gchamber@bright.net Toledo, OH

[✶ Re: Comments and corrections on Authenticode \(Atkinson, RISKS-18.85\)](#)

<Steve_Kilbane@cegelecproj.co.uk>

Wed, 5 Mar 1997 09:56:46 GMT

> As the architect and primary implementor of the Authenticode code-signing
> technology (boy, that'll get me mail :-)

It will indeed.

> found in Internet Explorer 3 and in
> Windows NT 4, I think my perhaps somewhat lengthy and clearly very biased
> perspective on some recent articles might be of interest to others.

Indeed. Good answers: calm, considered, and admitting that the rest of the

world both exists and has impact. It's a pity that Microsoft's (and other company's) press releases weren't so rational - it would stop rants like mine.

<Steve_Kilbane@cegelecproj.co.uk>

✂ Re: Comments and corrections on Authenticode (Atkinson, [RISKS-18.85](#))

Kevin McCurley <mccurley@swcp.com>

Wed, 5 Mar 1997 03:38:54 -0700 (MST)

I am sometimes reticent to discuss glaring security holes in public, but when a security mechanism is employed as a marketing tool, I believe it becomes fair game for criticism. Microsoft appears to have made a sincere effort to improve security with Authenticode, and Bob Atkinson gave a rather lucid explanation of the goals of Authenticode. Unfortunately, as a security mechanism, ActiveX with Authenticode has a rather big hole in it.

First, there are no mechanisms to prevent a web page from invoking the ActiveX components served by another page or already installed on the users disk. For several weeks the page at <http://www.digicrime.com/activex> was happily invoking an ActiveX component referenced and downloaded by clients from the Microsoft home page. When you loaded the page from DigiCrime with Microsoft Internet Explorer, you were presented with an official looking seal from

Microsoft certifying that the code you were about to install was written by them. And apparently it was. The second time you visited the page, the code was just invoked without warning. If you visited the Microsoft page first and then the DigiCrime page, the code from Microsoft was invoked without notice.

Second, ActiveX controls have no inherent protection from the problem of stack smashing, which is one of the most common forms of software security problems. The technique is rather technical, but the effect is that some programs can be caused to execute a sequence of instructions supplied by the argument to the program (via a web page). The technique is accomplished when an argument is used to overwrite fixed-length buffers allocated on the stack, depositing instructions on the stack. This technique is rather tedious to carry out, and does not work on all code. On the other hand, writing safe code is a very difficult task, and any code that uses standard C library calls like `gets()` or `sprintf()` to handle arguments is likely to be vulnerable. The technique has been well known to hackers for a long time, and has been used to abuse many Unix network programs, including `passwd`, `syslog`, `rdist`, `crontab`, NCSA's web server, `rlogin`, `talkd`, `mountd`, and `sendmail`. Note that Java is explicitly designed to prevent stack smashing.

Combining these two features of ActiveX, Authenticode becomes largely irrelevant. Code may be signed by the author, who was certified by a competent authority to be a reputable software developer. The

user reviews

the certification at install time, and accepts it on the basis of the reputation of the developer. The user then forgets about the code for some weeks to come. Later on, he or she visits a page of a hacker, or a page of a web site that has been broken into by a hacker, and invokes the code with arguments supplied by the hacker. The code may appear to do what it's supposed to, or appear to do nothing at all while it's erasing the web browser's history. The user may not even be aware that code is executing.

The user goes on to about 50 other pages that night, and shuts off their machine with no evidence of a problem. When they reboot they may have a huge problem, depending on what the code was reprogrammed to do. The Authenticode scenario suggests that the user can now call their lawyer to sue someone, but who do they sue? The hacker that the FBI can't track? The well intentioned but pressured software developer? The certification authority like Verisign that have forty page disclaimers of liability? Microsoft, who developed the ActiveX and Authenticode technology? None of the above I think. And even if someone could be sued, is this an acceptable substitute for having their machine work for their business?

My final criticism of Authenticode is unverified, in part because the public documents on the technique are rather vague. There appear to be no mechanisms for revocation of certificates that are already installed on machines. According to the document located at <http://www.microsoft.com/workshop/prog/security/authcode/>

[codesign.htm](#), the

default expiration date for Authenticode certificates is the year 2039, which means that no certificate should be expected to expire for a while.

If code is only re-verified when the certificate expires, then no buggy code will ever be replaced. If code is verified only at installation time, then this is even worse.

I should point out that none of this has happened in real life yet, in part because technologies like ActiveX are in their infancy and are not yet widely deployed. Once it's out there, I maintain that the problems will only be worse, as it is extremely difficult to keep track of the constant stream of security announcements. As I write this, Microsoft is scrambling to patch an unrelated security bug in MSIE 3.0 (see [Risks 18.85](#)). Clearly it's not unusual to ship code with serious security bugs, because every vendor is doing it in their haste to ship product.

It has been argued that the Java sandbox approach is too restrictive, and that "Users want and demand a rich computing experience". This may be true, but the rewards have to be something better than dancing bears in order to justify the risks. We take risks in life every day, but we do so on the basis of a continual risk/benefit analysis. Users may be willing to take the risks associated with network computing if they are presented with an accurate representation of the risk they are taking, and are given tools to manage and understand their risk. I can't see how Authenticode accomplishes this because

it represents an oversimplification of a very complicated subject. In addition, the move to integrate a user's desktop into the Internet will only lead to more confusion from users as they try to understand risks coming at them from all directions.

Kevin McCurley



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 18: Issue 87

Thursday 6 March 1997

Contents

- [ACM Kanellakis Award goes to public-key crypto creators](#)
[Peter G. Neumann](#)
- [Risks of mouse-based interfaces](#)
[Jay Hersh via Phil Agre's RRE](#)
- [Nevada May Ban Junk E-Mail](#)
[Edupage](#)
- ["New" Java hole](#)
[Gary McGraw](#)
- [Another view of what Bob Atkinson said on Authenticode](#)
[Christopher Rath](#)
- [An alarm-system code feature](#)
[Robert Orenstein](#)
- [SPAM generated from RISKS web site](#)
[Jim Thompson](#)
- [Re: Risk of IRS Outsourcing Processing](#)
[Pete Kaiser](#)
- [The number of the beast](#)
[Stu Savory](#)
- [Re: Tattooing SSNs on dogs to secure against dognapping?](#)
[Brian A. Reynolds](#)

- [Re: Not dead yet -- I'm still 3 degrees!](#)
[Bill Seurer](#)
 - [Re: Who made the call in the Moldova porn scam?](#)
[Aviel Rubin](#)
[Larry Kilgallen](#)
 - [AT&T "not responsible"?](#)
[Paul Colley](#)
 - [Fraudulent use of e-mail addresses](#)
[Andrej Panjkov](#)
 - [Re: Year 2K and my VCR: Dangers of Egg on Face](#)
[Nicholas C. Weaver](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✶ ACM Kanellakis Award goes to public-key crypto creators

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

Wed, 5 Mar 97 08:07:21 PST

At this week's ACM97, The Next 50 Years of Computing, the Association for Computing (ACM) has given its first Paris Kanellakis Theory and Practice Award to six people incisively involved in the creation of public-key cryptography: Leonard Adleman (University of Southern California), Whitfield Diffie (Sun Microsystems), Martin Hellman (Stanford University), Ralph Merkle (Xerox PARC), Ronald Rivest (MIT), and Adi Shamir (The Weizmann Institute of Science), ``for the conception and first effective realization of public-key cryptography. The idea of a public-key cryptosystem was a major conceptual breakthrough that continues to stimulate research to this day, and without it today's rapid growth of electronic commerce would have

been impossible.''

The award is named in memory of Paris Kanellakis, whose tragic death in December 1995 cut short a distinguished research career.

This event is most worthy of notice in RISKS, because the systematic use of public-key crypto has extraordinarily high potential for dramatically reducing many of the security risks so frequently discussed here -- including loss of confidentiality (e.g., through its use in the distribution of conventional crypto keys and in key management generally) and integrity (through its use in cryptographic checksums, digital signatures, and authentication). Congratulations!

⚡ Risks of mouse-based interfaces

Phil Agre <pagre@weber.ucsd.edu>
Wed, 5 Mar 1997 14:04:55 -0800 (PST)

[Once again the disability community takes the lead in decrying the GUI revolution, which has gone way too far. Interfaces should be measured in terms of how often one must move a hand from keyboard to mouse and back, in terms of the swapping delays that real users experience when endless little dialogue boxes have to pop up to accomplish anything, and in terms of the provision of meaningful keyboard equivalents for the functions that real people use. All the widespread PC OS's fail miserably at these criteria in my opinion. Except for a small number of crucial functions like

copy and
paste, I find myself being much more productive with a Unix
command
interface and my beloved Emacs text editor than with either the
Mac or
Windows interfaces and mouse- intensive WYSIWYG editors. Phil
Agre]

=====

This message was forwarded through the Red Rock Eater News
Service (RRE).

Send any replies to the original author, listed in the From:
field below.

You are welcome to send the message along to others but please
do not use

the "redirect" command. For information on RRE, including
instructions

for (un)subscribing, send an empty message to rre-help@weber.
ucsd.edu

=====

Date: Wed, 26 Feb 1997 12:24:37 -0500 (EST)

>From: "Jay Hersh aka Dr. Beer (SM)" <drbeer@doctorbeer.com>

To: voice-users@cuckoo.hpl.hp.com

Subject: Working with Quicken

I am currently using Quicken version 6 and previously used
version 5. What

I have found is that many of the "buttons" do not register their
names with

the Windows API and therefore DragonDictate can't automatically
build macros

on the fly to access these. This situation is worse with
Quicken 6 than it

was with version 5.

Overall I believe this is a significant problem within the
application

development industry, i.e. moving functionality more and more
towards mouse

oriented interfaces, using visual icons inside buttons rather

than plain
text and/or failing to register the text with the Windows API.
Additionally
more and more of the functionality of applications accessible
through mouse
usage lacks hot key equivalents making it difficult to create
macros by hand
(macros based on keystroke combinations are more reliable in
general than
those base on mouse positioning and button clicks since they are
independent
of window resizing).

Another obnoxious trend is that of popping up windows for each
bit of
functionality rather than subsuming them within the current
window. For
instance Quicken does an automatic backup which puts up 5
different windows,
one after another, each after you hit the enter key for the
current one.
This is annoying because you must wait each time for the new
window to map
onto the screen before you can hit the enter key. This also
makes
developing a macro to accomplish this difficult because of the
timing issues
involved in waiting for the next window to map before issuing
the next enter
key.

I believe that we as a community, along with Dragon Systems,
Kurzweil, and
IBM as companies need to stop these trends now. The more
applications
become developed around an assumption of the mouse as a primary
user
interface the more difficult utilizing the current generation of
speech
recognition technology (which is based upon synthetic keystroke
generation)
will become, and the more a barrier is presented to us and
especially to

those with severe enough handicaps that hands free usage is their only option.

Jay

This is a key free document, no keyboards were harmed in its creation. (The DragonDictate speech recognition system, the CIC handwriting recognizer, or some combination was used.)a

[Suggested to RISKS by "Mich Kabay [NCSA]"
<Mich_Kabay@compuserve.com>]

✶ Nevada May Ban Junk E-Mail (Edupage, 4 March 1997)

Edupage Editors <educom@elanor.oit.unc.edu>

Tue, 4 Mar 1997 12:05:50 -0500

The Nevada state Senate has introduced a bill that would make sending unsolicited ads directly to e-mail accounts a misdemeanor. "Most e-mail users pay for their service, so unsolicited e-mail is like receiving direct mail with postage due," says the Senate's majority leader, who notes the bill is modeled on a previous measure that bans unsolicited advertising over fax machines. California, Virginia and Connecticut are considering similar measures, but the Nevada legislature is widely viewed as closest to passing the ban. (*St. Petersburg Times*, 3 Mar 1997; Edupage, 4 March 1997)

⚡ "New" Java hole

Gary McGraw <gem@rstcorp.com>

Thu, 27 Feb 1997 16:40:59 -0500 (EST)

In a post to comp.lang.java.security and BUGTRAQ, Major Malfunction & Ben Laurie claimed on 25 Feb 1997 to have discovered a couple of new Java-based attacks. See:

<http://www.alcrypto.co.uk/java/>

The first "less serious hole" allows a miscreant "to gain access to information from the client machine which would normally be considered 'secure'." This works with the Netscape Navigator. Though their attack works as advertised on the page, there is really nothing new to this discovery. On their page, they say:

```
>All we can do is log the real identity of a client machine,
>despite
>most precautions they might take to prevent us from doing
>so... [firewalls, proxies, SOCKS, anonymizer...]
>we take one call to InetAddress.getLocalHost()...
```

And there you have it. Since the applet is running on the client machine and it is allowed to call `InetAddress.getLocalHost()`, it can find out the client machine's IP. Though this may surprise some users (especially those using the anonymizer), the ferreting-out of this information is not really a dangerous new invasion of privacy. The Web is currently not a private place. This demonstration serves to bring that point home. Your Browser is probably a blabbermouth. It is a clever move to use Java to look up an IP

at the client end through several proxy layers, but not all that clever.

The second attack is more disturbing. This one works only for the Microsoft Internet Explorer. They claim "this loophole allows an attacker to connect to any TCP/IP port on the client's machine." That's a bit of an overstatement, but interesting information about listening ports can be gathered (for possible later use). This may leave a firewalled host more susceptible to standard TCP/IP based attacks. That's bad.

The Java Security Manager usually disallows port scanning behavior. But the crackers use the well-known trick of sticking some Java code in the browser's cache and later executing it through a file: URL (using frames in the usual way.) Since Microsoft's cache layout is transparent, this attack works. This is an interesting variation on the Hopwood slash-and-burn attack described on page 69 of the book I wrote with Felten "Java Security: Hostile Applets, Holes, and Antidotes". The attackers cheat a bit for demonstration purposes by having the patsy clear their cache to begin with, but even without this exercise, guessing the cache location (one of four possibilities) would not be all that much of a challenge.

Contrary to the claim on their page, Java security rules are no longer relaxed for code loaded out of the cache (unless the cache happens to be in the CLASSPATH---not recommended). That problem was fixed. In any case, Microsoft apparently places HTML and class files in the same directory *stored with their original names*. Though MSIE can't browse

cache files directly, HTML pages can reference cache files by explicit name. Thus the file: URL, if properly constructed, can invoke the Java class. The applet the crackers stuff in your cache is a port scanner. In this case, the port scanning attack works because an applet is allowed to open a socket connection back to where it came from. Guess where it came from? The client machine. So a port scan is carried out by their cache-bomb applet.

That leaves only the problem of getting the port scan information back to the cracker site. They use the URL lookup covert channel to do this. (The Princeton team has explained this in a paper.) This is one of many ways of sending interesting tidbits out from an applet.

In summary, the information released on 25 Feb by Major Malfunction & Ben Laurie provides a couple of examples of some known attacks. If that helps educate Web users about the risks of executable content, that's good. If it stirs up unnecessary panic, that's bad.

Gary McGraw

p.s. See <http://www.rstcorp.com/java-security.html> for information on the book, Java Security: Hostile Applets, Holes, and Antidotes

Dr. Gary McGraw, Research Scientist, Reliable Software Technologies (RST)
Sterling, VA <<http://www.rstcorp.com/~gem>> gem@rstcorp.com

✶ Another view of what Bob Atkinson said on Authenticode ([RISKS-18.85](#))

"Christopher Rath" <crath@nortel.ca>

06 Mar 1997 07:20 EST

If I may be so bold as to re-state Bob Atkinson's arguments, here is my understanding of what he wrote:

Since the earliest days of the down-loading of software from BBSes, most users have typically down-loaded software just because it is there and they want to run it. Users have not refrained from down-loading and executing software because of security concerns.

Therefore, given that most users simply want to down-load and run whatever choice software offerings they encounter, Microsoft has endeavoured to make this process as transparent and unencumbered as possible.

In my view, Microsoft had two possible avenues of development and marketing to choose from, as they developed their browser: 1) to move the security benchmark forward, as Java has done, or 2) to leave it where it is, or even allow it to slip a bit, in order to garner market share and further control of network-based software interests. Is it, then, any wonder that they chose the latter!

The issues surrounding the consumer demand that Microsoft is responding to are the same issues which surround many other activities in society. To

state this another way, there are many pursuits which have risks associated with them, and large numbers of people choose, every year, to rationalize-away those potential risks; smoking, promiscuity, obesity, and many other socially acceptable behaviours are all examples of the same phenomena we see manifesting itself in the view Bob Atkinson propones.

Christopher Rath, Northern Telecom Ltd., Box 3511, Station `C',
Ottawa,
ONTARIO K1Y 4H7 CANADA crath@nortel.ca (613) 765-3141 FAX:
(613) 763-4101

⚡ An alarm-system code feature

Robert Orenstein <rlo@glyphic.com>

Tue, 4 Mar 1997 13:11:31 -0800

A friend of mine was going on vacation for a week, and asked me to come by her house each day to feed her cat. The house has a standard alarm system: when you open the door, it beeps; punch in the correct number and the beeping stops.

I memorized the code, but on the third day, I couldn't remember if the last digit was a 6 or a 7. I tried 7; the beeping stopped. I fed the cat and left. For the next two days, I punched in the same code, fed the cat, and left. On the last day, I punched in the code, fed the cat, and stayed around to read the paper. Five minutes later there was a knock on the door. It was the police.

They asked me if I lived there; I said I didn't, but was cat-

sitting. They asked me the address of the house I was in; I didn't know it, since my friend lives just around the corner from me and I know where the house is by sight, not by address. That was enough for them to assume that I was robbing the place; they handcuffed me and were about to take me to jail when a neighbor came out and verified that I was cat-sitting.

What had happened? The last digit of the alarm code was actually a 6, not a 7. But there's an additional "feature" of the system: if someone is pointing a gun to your head and telling you to turn off the alarm, you can simply add 1 to the alarm code and punch that in instead. This sends an "extreme distress" signal: the beeping stops as if you'd entered the correct code, but the police are dispatched to what they assume is a high-risk situation. I'd been sending false alarms for four days, but leaving before the police arrived.

The risks are clear: I could have been shot. As it was, my friend was billed for four false alarms; at \$50 per false alarm, it cost us \$200 (we split the bill).

Robert Orenstein

[Even though this item is marginally computer related, the design feature may be suggestive of related risks in authentication mechanisms -- especially those that seek to entrap attempted intruders. Incidentally, W.S. Gilbert was there before you: ``Either at sixes or at sevens.' ' PGN]

✉ SPAM generated from RISKS web site

Jim Thompson <jthomps@netcom.com>

Tue, 4 Mar 1997 14:10:47 -0600

The following bit of spam just arrived in the mail

>>>> "spam" == RHill <RHill@TheHost.com> writes:

```
spam> Hello, I saw your site at
spam> http://catless.ncl.ac.uk/Risks/17.78.html/, it looks
great...
```

The spam goes on to tell me how to register in Internet directories for a mere \$249. Note the reference to "your site" and the shallow compliment.

The "site" that the spammer refers to is RISKS Digest volume 17, issue 78; it contains a short contribution from me. Looks like the spammer grepped the web site for e-mail addresses, possibly in mail-to: tags.

Clearly e-mail spammers aren't any smarter or more discriminating than snail-mail spammers when it comes to gathering addresses; does this fellow really think that every mail-to: tag in a web page refers to its author(s)?

I'm reminded of the well-known junk mail that begins "Dear Mr. and Mrs.

Public Library, you have just won..."

Jim jim.thompson@pobox.com

✦ Re: Risk of IRS Outsourcing Processing (Pescatore, [RISKS-18.82](#))

<Kaiser@ACM.org>

Mon, 17 Feb 97 11:37:04 +0100

I believe that John understates the risk of outsourcing IRS forms processing, in several ways.

First, the government employees will continue to have access to the information, so the exposure of information doesn't simply shift from one venue to another, but continues at the first and is added at others, plus the risks of transporting the data first in hard format, then in electronic format. There will also be all the points of exposure in auditing the contractors.

Second, based on the behavior of the credit-reporting industry, private enterprise seems to show no very high standard of concern for privacy. The firms on which we rely for "preparing our tax returns, handling our checking accounts, or storing the records of counseling sessions" are individually responsible to us under law to maintain confidentiality, which gives them an incentive to act responsibly: if your accountant failed to safeguard your financial information, he could reasonably expect to find himself in court, with your personal lawyer at the other table. (Compare this to the record of the credit-reporting industry.) I doubt the same strict and direct responsibility would be found in outsourced processing of IRS forms, unless the IRS somehow magically could come up with a new and effective

set of
rules and operations to manage it, of a kind we have never yet
seen. The
RISKS item does little do allude to this.

The government employee's "little to fear as far as termination
of
employment" is a red herring, to which it's possible to oppose
another
scenario:

"Lowest Bidder, Inc." gets a big chunk of the IRS's outsourced
forms
processing business. Joseph Savvy, CEO of the business, knows
a potential
gold mine, and through friends in places where money is
laundered -- with
expert accountants and all the needed computing capacity --
does a lot of
data mining on the stream of information passing through his
business's
keyboards. This leads to a brand new stream of expert and
nearly
untraceable financial crime, plus other traditional crimes like
blackmail
and extortion, and the sale of some really exciting mailing
lists on the
open market. After all, who checks the provenance of
information on
mailing lists?

To me this seems not at all unrealistic.

Pete kaiser@acm.org

The number of the beast

Stu Savory <savory.pad@sni.de>

Wed, 05 Mar 1997 14:57:53 +0100

This is how dog tattoo numbers work in Germany, which your other SSN-reporter may care to adopt.

Our dog has a 4-digit number tattooed in its ear. A finder can call the registry centre (number available at each local vet or attached elsewhere to the dog) and report e.g., Hellhound 0666 found. The registry centre database may report several different dogs 0666, so additional data about gender and breed may be asked for, for clarification. If you are on the owner short-list, you get a phone call, asking whether your dog is missing. If so, you are given the phone number/address of the finder. Lazy finders just turn the dog into the local pound & let them sort it out (maybe missing on the chance of a reward).

Because dogs are required to be numbered, either per tattoo or per subcutaneous transponder, for crossing national borders, this mechanism is no extra hassle. Probably UK does not have this border requirement.

Stu Savory (Owner, Bulldogs 0157 and (yes!) 0666)

[They have Border Collies instead, whose collars enable Collie forwarding and Collie flowering. However, we are wandering, so let's terminate the ssnaggy dog stories. PGN]

⚡ Re: Tattooing SSNs on dogs to secure against dognapping?

"Brian A. Reynolds" <bareynol@cca.rockwell.com>

Wed, 05 Mar 1997 10:22:53 -0600

It is common practice to engrave one's drivers license number onto object which are likely to be stolen. This assists in the identification and retrieval. Guess what? In Iowa, the Drivers License number is identical to one's SSN! So the risk is in assuming that your SSN is privileged information. It gets written on every check that I write, it's also my health care member ID number, employee identification number, etc. etc. etc.

Brian Reynolds

⚡ Re: Not dead yet -- I'm still 3 degrees!

Bill Seurer <seurer@VNET.IBM.COM>

Tue, 4 Mar 1997 14:34:55 -0600 (CST)

> She replied, "3's an error code."

On a medical device with 4 digits output what sort of meaningful error code would you expect? Our home model does the same thing (although it flashes the result for an error) and its manual clearly states what each error code means. It also explains how to use it to avoid getting the various errors.

Error "3" is that it couldn't read your temperature, usually a result of not aiming it properly. I don't think anyone would confuse that with a valid reading.

The risk here seems to be that the nurse was not trained beyond "stick it in the ear and push the button". Sort of like if she had been

trained with an oral thermometer to "stick it in the mouth" and not properly to place it under the tongue. At least the aural thermometer (is that what they are called?) tells you there's a problem whereas the oral one would just give a bad reading. They also work vastly better for "difficult" patients like small kids.

Bill Seurer ID Tools and Compiler Development IBM
Rochester, MN
BillSeurer@vnet.ibm.com <http://members.aol.com/BillSeurer/>

✶ Re: Who made the call in the Moldova porn scam?

Aviel Rubin <rubin@quip.eecs.umich.edu>
22 Feb 1997 16:32:16 GMT

A colleague of mine at AT&T suggested that this is similar to someone breaking into your house and making international calls. Who is responsible? Actually, I think it's more like someone knocking on your door, you let them in, and when you are not paying attention, they make these calls. Now, who is responsible? You? The phone company? Your house insurance?

Although I hate to see people defrauded, I have been waiting for the day that people get burned from downloading programs from the net and running them. How can you expect anything else? Hopefully this publicity will help educate people against these dangers.

Avi Rubin [usual disclaimers apply]

⚡ **Re: Who made the call in the Moldova porn scam? (Horowitz, [R 18.84](#))**

"Larry Kilgallen, LJK Software" <KILGALLEN@Eisner.DECUS.Org>
Sat, 22 Feb 1997 14:40:09 -0500 (EST)

Perhaps phone lines should be password protected. That is available for incoming WATS calls. I have a simpler form for outgoing calls -- it is only one digit long and the password is "9". Only the most diligent of the scam artists would bother with this possibility. Even safer are the minority of folks whose password for an outside line is "7" or some other non-9 digit. Scam artists who bother taking that into account must be really rare, and deserving of being hired into an honorable (?) position fixing some of the commercial software so often discussed in RISKS.

Larry Kilgallen

⚡ **AT&T "not responsible"?**

Paul Colley <colley@qucis.queensu.ca>
Sat, 22 Feb 1997 10:08:43 -0500

>From: Marc Horowitz <marc@cygnus.com>
>Subject: Re: Who made the call in the Moldova porn scam?
(Claar, [RISKS-18.83](#))

>... A more proper analogy: If someone steals your car, and

crashes it into

>another car, totalling both, the owner of the other car is not responsible.

>If someone steals your phone line and makes lots of calls, AT&T is not

>responsible.

I'm not unhappy with your conclusion, but I strongly dislike your analogy.

International calls are very profitable for phone companies. If someone

steals your phone line and makes lots of international calls that AT&T can

collect for, AT&T makes a substantial profit---and unlike the car accident

analogy, doesn't risk lethal injury.

This makes it to AT&T's benefit to be a "bad driver", to encourage as much

damage and mayhem on the "road" as possible. Bad analogy; bad policy.

There is good reason to hold AT&T responsible for calls made to that number

after AT&T was notified of the scam; and good reason to hold the customers

responsible before that point.

Paul Colley colley@qucis.queensu.ca +1 613 545 3807

<http://www.qucis.queensu.ca/home/colley/info.html>

⚡ Fraudulent use of e-mail addresses

Andrej Panjkov <A.Panjkov@latrobe.edu.au>

Tue, 4 Mar 1997 10:55:11 +1000

A recent item on fraudulent Usenet postings reminded me of a stunt some of

my students pulled on me a couple of years ago.

It seems that some students (we never found out who) posted some personal ads purporting to come from me on a romance web page. I found out about this when I received e-mail from some admirers. My wife was unimpressed. :>

We traced the source of the forged messages to an undergraduate computer study hall. They have since changed their policy to require that users obtain accounts first.

It took a whole week before the fraudulent message was removed from the web page it was on, and then only when I threatened to report the owner of the page to whatever authority governed fraudulent communications in their jurisdiction.

The responses I received to "my" ad were from some quite charming ladies who were also victims of this scam. I regarded the matter as a prank, but the same technique could have been used to place my name in uglier contexts

Lessons: monitor undergraduate computers carefully. At the very least, register users. And use PGP. Perhaps, we should all periodically sweep the web to see where our names are ending up?

Dr Andrej Panjkov, La Trobe Uni, Melbourne, Australia A.
Panjkov@latrobe.edu.au
<http://guardian.maths.latrobe.edu.au> +61 3 9479 2595

⚡ Re: Year 2K and my VCR: Dangers of Egg on Face ([RISKS-18.84](#))

"Nicholas C. Weaver" <nweaver@CS.Berkeley.EDU>
Thu, 27 Feb 1997 17:45:49 -0800 (PST)

Upon further testing (prodded by others), I poked around on my VCR and, well, it does have the proper calendar, although the date is shown wrong, only the year is affected. It gets the days right (Feb 29 2000 is a tues, and the VCR agrees).

I guess the risk is worrying about non-problems when there are much important things.



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 18: Issue 88

Friday 7 March 1997

Contents

- [NASA: Another Website Bites the Dust](#)
[David Kennedy](#)
- [Two More Microsoft Internet Explorer Bugs](#)
[David Kennedy](#)
- [Another MacInTax "Glitch"](#)
[David Kennedy](#)
- [Re: 12/99 problem](#)
[Clive D.W. Feather](#)
[Mark Brader](#)
- [Computer glitch leads to police friendly fire](#)
[J.R.Valverde jr](#)
- [Re: Mouse-based interfaces](#)
[Dean Esmay via Phil Agre](#)
- [Trusting the software vendor](#)
[Matt Welsh](#)
- ["Rich" computing versus security](#)
[Matt Welsh](#)
- [Re: ActiveX security: The other side](#)
[Wayne K. Gerdes](#)
- [Lab monitoring](#)

[Fritz Schneider](#)

● [Risks of crying wolf](#)

[David Lesher](#)

● [Moonlighting on safety-critical systems](#)

[Jonathan Bowen](#)

● [The SEI Conference on Risk Management](#)

[Carol Biesecker](#)

● [The Ethics of Electronic Information in the 21st Century](#)

[Les Pourciau](#)

● [Info on RISKS \(comp.risks\)](#)

✂ NASA: Another Website Bites the Dust

David Kennedy <76702.3557@compuserve.com>

Wed, 5 Mar 1997 16:59:16 -0500

<http://www.nasa.gov> is NASA's home page. It appears it was hacked last night. It's off-line now. When a mirror of the hacked page is posted, I'll let you know if someone else on the list doesn't first.

If my report is accurate, the hacked page included:

```
>Our mission is to continue where our colleagues the ILF left
>off. During the next month, we the members of H4G1S, will be
>launching an attack on corporate America. All who profit from
>the misuse of the internet
```

"ILF" refers to the Internet Liberation Front who attacked GE and others in December 94. The only person who has claimed to be a member of the ILF is Christopher Schanot, a then-high schooler from St. Louis, who's in jail for what he did. He broke into systems using a password provided by a classmate who was the son of an employee of one of the systems he entered. He also

used password sniffers to capture legitimate passwords that were passed over the net unencrypted.

The rest of the hacked NASA page is some mundane pro-hacker stuff about Kevin "Condor" Mitnick and Ed "Bernie S" Cummings.

Lesson: Running a web site requires somebody to take the time to know about the vulnerabilities and *do* something about them. There are no quick fixes. As William Hugh Murray, a colleague, says, "There is no magic."

Dave Kennedy CISSP National Computer Security Assoc
76702.3557@compuserve.com

🔥 Two More Microsoft Internet Explorer Bugs

David Kennedy <76702.3557@compuserve.com>

Fri, 7 Mar 1997 02:12:18 -0500

1. EliaShim warns of security hole in Internet Explorer
Courtesy of the COMTEX Newswire via CompuServe's Executive News Service

> PC Week Online (March 6, 1997) - Less than a week after the discovery of a
> potential security gap in Internet Explorer 4.0, Microsoft Corp. may have
> another hole to fill. EliaShim Ltd., an anti-virus company, claims it has
> identified security problems in Microsoft Internet Mail and News
> applications. "Hostile links" can be embedded in newsgroup messages or in
> messages received by Internet Mail as shortcuts, company officials said.

2. Another Internet Explorer Bug Found

Courtesy of the COMTEX Newswire via CompuServe's Executive News Service

> REDMOND, WASHINGTON, U.S.A., 1997 MAR 7 (Newsbytes) -- By Bob Woods.

> Another bug in Microsoft's [NASDAQ:MSFT] Internet Explorer (IE) World Wide

> Web browsing software has been discovered by a group of University of

> Maryland students. The students posted their results at their Web site

> today, and claimed that the bug could let a hacker remotely break into a

> user's computer or install viruses onto the system. UMD students David

> Ross, Dennis Cheng, and Asher Kobin found the bug in IE 3.01.

Microsoft acknowledges the bug but hasn't defined its full impact.

> The bug apparently centers around IE's IFRAME, or floating frames feature.

The patch for the URL/LNK bug does not fix the UMD student's bug.

> The students' Web site is at <http://dec.dorm.umd.edu/> .

> Microsoft's IE site is at <http://www.microsoft.com/ie> .

Dave Kennedy [CISSP] Research Team Chief, National Computer Security Assoc.

⚡ Another MacInTax "Glitch"

David Kennedy <76702.3557@compuserve.com>

Fri, 7 Mar 1997 02:12:21 -0500

Intuit warns of MacInTax glitch

Courtesy of the COMTEX Newswire via CompuServe's Executive News

Service:

> MacWEEK Online (March 5, 1997) - Intuit Inc. this week sent a letter to
> its MacInTax users detailing a potential pitfall for electronic
> filers. Users who fail to save their documents before filing them
> electronically may receive word from the IRS of an incomplete filing. The
> company said the problem will likely affect only a small percentage of
> users, as most would opt to save their work before transmitting
> files. However, there are some customers who tend to go straight to the
> electronic filing function without saving.

Patch at <http://www.intuit.com/> or by disk.

> In a statement, Intuit Vice President Larry Wolfe said the problem is
> "absolutely covered" under Intuit's general product guarantee. "If a
> customer has filed an incomplete electronic return with MacInTax, Intuit
> will pay the penalty plus any interest assessed by the IRS," he said.

Dave Kennedy [CISSP] Research Team Chief, National Computer Security Assoc.

✶ Re: 12/99 problem

"Clive D.W. Feather" <clive@demon.net>

Fri, 7 Mar 1997 08:19:07 +0000

This looked like a Y2K problem at first sight. However, it isn't. Some names are changed to protect me from defamation suits.

I work for a major ISP, and many of our customers pay us monthly by credit card. This problem hit a whole batch of customers at once, but I'll just pick one and call him or her. C has a card issued by a major bank, who we'll call B. We use a major credit card organisation in the UK for all credit card transactions; let's call them V.

When a customer signs up with us, they quote card number and expiry date, which we enter on to our computer. Each month we take that data and send V a packet of the form <amount, card number, expiry>. Now suppose that the card originally expired in 08/96. The customer might be good enough to let us know that they have a new card expiring in 08/98, and we can update our records, or they might not. If they don't, then we send <amount, card number, "12/99"> to V.

The other day we charged C's card. It came back "rejected". So, following normal practice, we suspended the account and waited for C to call us. After doing so, C phoned B and confirmed the card was fine. A four-way conversation then ensued. It turns out that what happened was the following.

C's card had an original expiry date of 12/96. Our software noticed that the card was expired, and sent the request with an expiry of 12/99. On arrival at V, their software looked up the card number in a table which says, in effect: "this range of card numbers was issued by B with an expiry of 12/96". V's software also knows that B uses a 3-year rollover of cards. So they added 3 to 12/96, amended the expiry field to 12/99, and

forwarded the
request to B.

Meanwhile, someone at B decided that, given the special meaning of 12/99, issuing cards that expiry then is a Bad Thing. So cards expiring in 12/96 were renewed with an expiry of *11*/99. The resulting mismatch caused the rejection.

I understand that V's computers will be reprogrammed to solve this problem. But just whose is the error?

Clive D.W. Feather Demon Internet Ltd. <clive@demon.net> +44
181 371 1138
CityScape Internet Services Ltd. <cdwf@cityscape.co.uk>

⚡ Re: 12/99 problem

<msb@sq.com>

Fri, 7 Mar 97 11:11:44 EST

Clive Feather writes:

> This looked like a Y2K problem at first sight. However, it isn't.

Sure it is. Without Y2K, who would have thought of choosing the month/year

"12/99" as an out-of-band flag value? In fact it's a particularly silly

Y2K error, since 99/99 would have fitted the field length just as well.

> But just whose is the error ?

Either B's or V's, but in order to tell which, we'd have to know

what they
said to each other and when. Did V tell B that they needed to
know their
expiry rollover pattern in order to validate transactions, or
did they just
assume that because B had been using a 3-year rollover they
always would?
If the former, then did B inform V that their practice was being
varied this
time, and if so, did they do it in timely manner so that V could
be prepared
for it?

Mark Brader, msb@sq.com SoftQuad Inc., Toronto

⚡ Computer glitch leads to police friendly fire

"J.R.Valverde (jr)" <jrvalverde@samba.cnb.uam.es>

Fri, 07 Mar 1997 18:30:08 WET

The Vasque Country in the north of Spain has a strong terrorist
group, ETA,
which -among other activities- often attacks the Police.

Last week there was a sad incident: two secret police groups
started
shooting each other. The reason? According to the government it
was all due
to a computer glitch.

Things are said to happen like this: that afternoon there had
been a bombing
in town. One group of civil-dressed secret policemen saw a group
of armed
guys in a car and started off after them. Of course, first thing
they did
was call the central offices to ask for information on the car
and its
owner. Here comes the computer bug: they could not get any
information and

assumed those guys were the terrorists that had done the bombing.

The other car was loaded with secret policemen too. They saw that they were being followed by armed civil-dressed people in a car, could not get any information either and assumed they were being pursued by terrorists that were after them to kill them in a second coup de main and fled away.

You can see what happened. At some point the first car stopped, the second did the same, all them took their arms, all them got alarmed at seeing each too their arms, someone shoot first, and hell was left loose...

The problem? relying on computers for tasks where human lifes are involved and not having adequate fail-safe systems.

jr

🔥 Mouse-based interfaces (Re: Hersh, [RISKS-18.87](#))

Phil Agre <pagre@weber.ucsd.edu>

Thu, 6 Mar 1997 19:01:15 -0800 (PST)

[He's right. Phil]

=====
=====

This message was forwarded through the Red Rock Eater News Service (RRE).

Send any replies to the original author, listed in the From: field below.

You are welcome to send the message along to others but please do not use the "redirect" command. For information on RRE, including

instructions

for (un)subscribing, send an empty message to rre-help@weber.
ucsd.edu

=====

Date: Thu, 6 Mar 1997 21:53:39 -0500
>From: Dean Esmay <esmay@syndicomm.com>
Subject: mouse-based interfaces

[...]

I was both pleased and disturbed to read Jay Hersh's comments on
GUIs and
the disability community in your recent RRE mailing, and a bit
concerned
about some of your comments on his thoughts. Not that either of
you are
wrong, but you aren't exactly right either.

The deaf child, the woman with multiple sclerosis, and the blind
man all
have fundamentally different needs, none of which are necessarily
compatible. Given that, I'm not sure who Jay Hersh thinks he's
talking
about when he refers to the "community" needing to fight against
mouse-centric interfaces, and I am even less sure that the
waters aren't
further muddied by your comments about the efficiency of keyboard
interfaces.

I worked for a number of years in an employment agency for the
disabled, and
have attended and even led workshops on how to make computers
more
accessible to the disabled. I think three things should be kept
in mind
before anyone tries to influence how computers interact with
people:

- 1) GUIs are substantially beneficial to some disabled users.
- 2) The problem with computer software not working well for some

people has
been around far longer than the widespread use of GUIs.

3) There is no one solution (to date) that works well for everybody.

Prior to GUIs, the visually impaired did pretty darned well. After all, text-based software can often be easily adapted to speech synthesis. While there were things to complain about, the blind generally did pretty good. But the blind are not the only members of the disability community, and the non-blind disabled were often still faced with serious aggravations, or even locked out in the cold. GUIs fixed that for many of them.

A number of devices exist that substitute for the traditional mouse, the best of which is a strap-on headset with which a person with no use of hands can point by merely moving her head (or even just her tongue if neck mobility is limited) and "clicking" with a puff of breath. Your beloved EMACS is normally worthless to a woman without arms. But give her an interface where she can point and click with her hands-free mouse, "type" clicking on the keys of a floating on-screen keyboard that feeds her "keystrokes" to the window of her choice, and that responds to specific voice commands for shortcuts, and she can do anything you can. In today's GUI world, most properly-written software can use such special tools without need for modification or special programming.

It's also probably unfair to lump Apple in with Microsoft. Apple has a long history of working with the disability community. Back in the

old Apple II

days, they manufactured special devices to help the disabled use their

computers. When the Mac came along, they cooperated enthusiastically with

the manufacturers of the hands-free mouse and similar devices, and worked

hard to make their GUI and their API work effortlessly with such special

tools. Apple also put a good bit of money into developing and testing

their Easy Access and Closeview extensions, which ship free with every

Mac/OS machine and vastly improve the interface for many disabled people

(including some with partial vision). They even include system software

extensions to make voice control possible in any program, and powerful

built-in scripting that can automate many tasks in many applications.

Of course, Apple comes up short with some, especially the blind. That

section of the community has generally stayed with the text interface

operating systems that work best for them. But still, Apple has arguably

done much to adapt to people with special needs, for which they deserve

credit.

But let's set aside Apple, which is only one imperfect company. The fact is

that today, a majority of the disabled can use much Windows software right

off the shelf, too. This is a tremendous step forward from ten years ago.

But the same GUI which has helped so many others is forcing the blind to the

sidelines. It's damned hard to adapt a GUI to a speech-synthesized,

sight-free world. It's not impossible; some very clever macro-

based

work-arounds do exist. But much more needs to be done to address this problem.

There badly needs to be a widespread discussion of issues like applications and APIs which just plain ignore the needs of the disabled. We need to encourage elimination of unnecessary popup menus and dialogs, buttons with graphics but no text, buttons with text but no graphics, hierarchical pull-down/pop-up menus that are a bitch to navigate if you can't see well or have poor coordination, and more. The blind also have a need for more productivity and utility software written specifically with them in mind; the market is large enough now that, while it might not be much of a blip on Microsoft's radar screens, it's more than enough for small cottage industrialists to make decent money. I've met a few people who write that kind of software for a living, but there's room for more.

I commend you for bringing this issue to wider attention, and I hope you'll talk more about it in Red Rock Eater. But I urge you not to get lost in generalizations about what a vague, unspecified "disability community" needs, or tangle that up with what you find most useful for yourself.

In any case, thanks for doing something to at least start people thinking about these issues!

<http://www.syndicomm.com/esmay>

✉ **Trusting the software vendor (Re: Atkinson, [RISKS-18.85](#))**

Matt Welsh <mdw24@cl.cam.ac.uk>

7 Mar 1997 12:09:01 GMT

> ... you trust the retailer to sell you only legitimate product ...

It's interesting that Microsoft should defend Authenticode with this analogy, when in fact Microsoft itself has been known to distribute CD-ROMs with viruses. Given that I can't even "trust" Microsoft software obtained through traditional distribution channels, by what stretch of belief am I supposed to concede that Authenticode will solve this problem for non-traditional channels?

M. Welsh, Cambridge Computer Laboratory

✉ **"Rich" computing versus security (Re: Atkinson, [RISKS-18.85](#))**

Matt Welsh <mdw24@cl.cam.ac.uk>

7 Mar 1997 12:24:05 GMT

>Users want and demand a rich computing experience. ...

It seems that it would be worthwhile in the course of this discussion to step back a bit -- instead of merely attacking or defending Authenticode, why don't we look at the basic statement used to defend ActiveX? Paraphrasing, "In order to have a rich computing experience, applications must forgo some degree of security."

This is a contentious statement. A great deal of work has been done in both the academic and industrial computing communities to develop computing environments which enable 'sandboxing' of code and still provide a 'rich computing experience' - e.g., flashy graphics, I/O device and network access, and the like. Although with the advent of Java we are starting to see these ideas in the mainstream, they're not particularly new.

It is far easier to verify and trust my Java Virtual Machine implementation, for example, than it is to verify and trust every ActiveX control which comes my way. In the former case we are basing our trust on the developers of the computing environment - in the latter, upon every software developer who ever writes or has a hand in every ActiveX control we use. In the former case, the security of the system can be verified and is enforced through technical means; in the latter, only through social and legal ones. I know which one of these I'd rather employ.

M. Welsh, Cambridge Computer Laboratory

✉ Re: ActiveX security: The other side (Rath, [RISKS-18.87](#))

"Wayne K. Gerdes" <w.k.gerdes@larc.nasa.gov>
Fri, 07 Mar 1997 11:29:56 -0500

Having done a proposal for development of a worm/agent based software distribution system similar to ActiveX or FTP inc's CyberAgent I

have done
some serious thinking about the security problems. A truly
useful piece of
software must have access similar to a standard user account, or
at least a
captive account. Java's sandbox model is wonderful if the idea
is to
provide graphics using the local machine's CPU power. It is,
however, very
difficult to perform useful work with such a system, where
useful work is
defined as, say word processing involving references to active
objects and
saving files locally. A more scientific example might be
performing
calculations as part of a distributed computation and forwarding
the results
to some arbitrary destination. Another example might be
querying a series
of remote databases and forwarding the results. These examples
require the
ability to address arbitrary hosts, require disk storage space,
and/or a
variety of other access and privileges. The primary problem is
that Windows
3.1 thru Windows 95 does not have the security features to
isolate such
programs. Under "more advanced" operating systems such as UNIX,
VMS, or
Windows NT, to name just a few, it is possible to create a
"larger sandbox",
via separate accounts, captive accounts, disk quotas, limiting
system calls,
etc. Note that even this will not eliminate the security problem
(s). It is
always the temptation to install new software with root
privilege or
equivalent. It is almost always possible for hackers to find
some OS bug to
exploit. As readers of this digest know, even well intentioned
programs
often corrupt data, crash machines etc.

The next element of the security problem, is the surprisingly high quality of web distributed software. Despite the many security concerns of downloading and executing some arbitrary piece of software written by Unknown, most people do it and the worst thing that usually happens is that it crashes. As Mr. Rath notes, most people want to "just get on with it". Security warning messages about "Should this program be allowed to access the disk?" or "Accept this cookie?" quickly become annoying and get turned off. Under these circumstances the current digital certificate and code signing is a reasonable approach. What the current system does lack is degrees of trust. It might be reasonable to require a very large bond before issuing a AAA certificate and a small one for a BBB certificate. Web sites could be established to rate the reliability of new software. Something like Cancel Moose could be developed to chase down and deactivate certificates belonging to errant software. Instead of downloading certificates they might be implemented as active objects stored at well known web sites. This would make the process of revoking them MUCH easier.

Looked at from this view point ActiveX vs Java can be seen as sort of large scale beta testing of "the REAL solution".

Wayne K. Gerdes w.k.gerdes@larc.nasa.gov (757)864-1520 (AST,
Data Systems)
Flight Electronics Tec. Div, Systems Integration Branch MS 152D

✶ Lab monitoring (Re: Fraudulent use of e-mail addresses, RISKS-18.87)

Fritz Schneider <fritz@columbia.edu>

Fri, 7 Mar 1997 17:10:47 -0500 (EST)

Just a quick response to Andrej Panjkov's article regarding a bad experience he had with e-mail forged in his name. After relating his situation, Mr Panjkov gives the following advice:

```
> Lessons: monitor undergraduate computers carefully. At the
> very least,
> register users. And use PGP. Perhaps, we should all
> periodically sweep
> the web to see where our names are ending up?
```

Although in theory I agree with all of these suggestions (ignoring the impracticality of the last), I question the wisdom of assuming that misuse of technology such as the net will be perpetrated by the younger generation.

There is no reason to necessarily suppose that older (graduate) students are any more ethical than their younger (undergraduate) counterparts. In fact, it seems to me that the BIGGEST risk comes from those with more education, skills, and experience. Therefore if one can only monitor one lab but not both, it would be more prudent to keep an eye on those with the resources to carry out the most destructive acts.

I am, however, not convinced that mere "monitoring" of a computer lab can prevent forged e-mail...

The Risk here: 1. Assuming that age/education is inversely proportional to ill intent.

Fritz Schneider [fritz@columbia.edu]

✦ Risks of crying wolf

David Leshar <wb8foz@netcom.com>

Fri, 7 Mar 1997 04:48:27 GMT

I am in Maryland [301], but the local calling area extends across DC [202] into Virginia[703]. Within that area (which also includes parts of 410 and soon will have 240 and 443), calls are 10D, with a leading "1" not necessary. (Rather; without it, you are assured the call is not toll.)

So I tried to call 703 715 xxxx, in the Vienna area. But I got an intercept, telling me that THAT number was now in the 540. (540 was split from 703 last year, with Risks of its own after Bell sent postcards to the WRONG group of customers...)

Now, AFAIK, no part of 540 is DC-Metro. And 715 did not move. But I gave it a try, and sure enough, Bell decided "540-715X" was a 301 #, (Gaithersburg, local to me) but one out of service. (With no "1" it knew better than to try 540-715-xxxx.)

Now, 715 is **still** in 703. So that intercept is bogus. But look who likely gets wrong numbers from believing it: 540-715 if/when it's created, and 301 540-715x.

The Risks? Well, believing the error message may do you more harm than good. And as the sparse NPA space turns increasingly dense,

others won't
have the benefit that I received; that of the wrong number I
dialed being
idle.

Did Arthur C. Clarke see THIS coming, too ;-?

wb8foz@nrk.com (301) 56-LINUX

🔥 Moonlighting on safety-critical systems

Jonathan Bowen <J.P.Bowen@reading.ac.uk>

Fri, 7 Mar 1997 09:24:45 GMT

Below is a possibly worrying message which I received recently.
(Name and
contact details are blanked out.) Who takes the responsibility
if things go
wrong?

Jonathan Bowen, Univ. of Reading, Department of Computer
Science, Whiteknights,
PO Box 225, Reading, Berks RG6 6AY, UK [http://www.cs.reading.ac.
uk/people/jpb/](http://www.cs.reading.ac.uk/people/jpb/)

>Date: Thu, 6 Mar 1997 19:05:30 +0000
>From: xxxxxxxx <xxxxxxx>
>To: J.P.Bowen@reading.ac.uk
>Subject: wanted

>Would it be appropriate for you to [post] this opportunity on
your system?

> WANTED - Moonlighter with mixed signal simulator and formal
verification
> tools to modify a circuit for a medical device. Reply
confidentially to
> FAX xxx xxx xxxx.

✦ The SEI Conference on Risk Management

Carol Biesecker <cb@SEI.CMU.EDU>

6 Mar 1997 18:54:32 GMT

The SEI Conference on Risk Management:

Managing Uncertainty in a Changing World

April 7-9, 1997, The Cavalier Hotel, Virginia Beach, Virginia

For the most current information about the SEI Conference on Risk Management and other SEI events, visit our Web site at www.sei.cmu.edu/products/calendar.html

For additional information about the conference, contact

SEI Customer Relations

Software Engineering Institute

Carnegie Mellon University

Pittsburgh, PA 15213

Phone, Voice Mail, and On-Demand FAX

412 / 268-5800

E-mail: customer-relations@sei.cmu.edu

World Wide Web: <http://www.sei.cmu.edu>

The keynote speakers are

. Dr. Paul G. Kaminski, Undersecretary of Defense Acquisition and Technology

. General Alton D. Slay, USAF (ret), Slay Enterprises, Inc.

. Timothy Lister, The Atlantic Systems Guild, Inc.

Five half-day tutorials are being offered during the morning of Monday, April

7, 1997.

Two panel sessions are planned for the afternoon of Tuesday, April 8, and

the morning of Wednesday, April 9.

A special track is planned for invited program managers to talk about

their risk management experiences. This track starts Monday afternoon,

April 7, 1997, and runs in parallel with two more tracks, Acquisition/Risk

Management in Practice and Theory, Models, and Lessons Learned.

✦ The Ethics of Electronic Information in the 21st Century

Les Pourciau at UMem <POURCIAU@MSUVX1.MEMPHIS.EDU>

Fri, 07 Mar 1997 09:02:55 -0600 (CST)

THE ETHICS OF ELECTRONIC INFORMATION IN THE 21st CENTURY
September 26-28, 1997

The University of Memphis {Libraries & Information systems &
Linder Center

for Urban Journalism & Division of Research and Graduate
School & Marcus

Orr Center for the Humanities & Cecil C. Humphreys School of
Law &

Fogelman College of Business and Economics }

Fogelman Executive Center, The University of Memphis, Memphis
TN, U.S.A.

http://www.people.memphis.edu/~operations/fec_list.htmlx

Additional Memphis Web Site: <http://www.memphistravel.com>

Abstracts due by 25 April 1997. [Check website for details.]



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 18: Issue 89

Wednesday 12 March 1997

Contents

- [President's Commission on Critical Infrastructure Protection](#)
[PCCIP](#)
- [Alberta Stock Exchange Shuts Down](#)
[Mich Kabay](#)
- [Hot and cold running randomness](#)
[Dan Wing](#)
- [Vietnam will censor Internet content](#)
[David Farber](#)
- [More RISKS-relevant ACM awards](#)
[PGN](#)
- [The Ariane 5 explosion: a software engineer's view](#)
[Robert L. Baber](#)
- [Usability and Security re: Authenticode](#)
[Mary Ellen Zurko](#)
- [CaptiveX/Authenticode](#)
[Henry G. Baker](#)
- [Continual Risk/Benefit Analysis](#)
[Benedikt Stockebrand](#)
- [Re: Trusting the software vendor](#)
[David Collier-Brown](#)

[Daniel Hicks](#)

● [ActiveX Security for Dummies](#)

[Peter Gutmann](#)

● [The real goal of Authenticode](#)

[Mark Seecof](#)

● [CFP: DIMACS Workshop on Formal Verification of Security Protocols](#)

[Catherine A. Meadows](#)

● [Info on RISKS \(comp.risks\)](#)

✶ **President's Commission on Critical Infrastructure Protection**

"The President's Commission" <COMMENTS@PCCIP.GOV>

Thu, 27 Feb 1997 13:01:29 -0500

The President's Commission on Critical Infrastructure Protection (PCCIP)

advises and assists the President of the United States by recommending a national strategy for protecting and assuring critical infrastructures:

telecommunications, transportation, electric power, oil and gas, banking and finance, water, emergency services and continuity of government services.

The PCCIP Web site contains background on the Commission and information about its activities and mission.

The site's home page may be accessed at <URL:<http://www.pccip.gov/>>.

Submitted to RISKS by the PCCIP Comments Desk, comments@pccip.gov

[The Commission is now in full swing. Seven of the commissioners plus some staff members attended a Workshop on Protecting and Assuring Critical National Infrastructure at Stanford University on 10-11 Mar

1997,

sponsored by the Stanford University Center for International Security and

Arms Control and co-sponsored by the LLNL Center for Global Security

Research. Many other luminaries also participated (e.g., Bill Perry --

former co-director of CISAC and former SecDef). For more information on

this and earlier CISAC workshops, contact Sy Goodman, Center for

International Security and Arms Control, 320 Galvez, Stanford University,

Stanford, CA 94305-6165 <sgoodman@leland.stanford.edu>. Sy hopes they

will have two reports on the most recent workshop out in a couple of

months. The workshop was a feast for the various RISKS devotees who had

been invited. (Note: Sy is a member of the ACM CCPP group that sponsors

RISKS.) PGN]

✶ Alberta Stock Exchange Shuts Down

"Mich Kabay [NCSA]" <Mich_Kabay@compuserve.com>

Wed, 12 Mar 1997 12:49:40 -0500

Angela Barnes and Brent Chang of the **Globe and Mail** ("Canada's National Newspaper") report today (97.03.12, p. B1) that (quoting):

`For the second time in six sessions and the third time this year, the Alberta Stock Exchange has lost a day of trading because of problems with its leading-edge computerized trading system.'

The authors make the following key points:

- * System failure occurred at opening of trading on 97.03.11 at 07:30 MST.
- * Technicians worked until 13:00 and tried to restart software but programs failed immediately.
- * Bug fixes continued all night.
- * Previous software errors stopped trading on the ASE for an entire day on 4 March and during January; two other day-long halts occurred between in 1996 after the software went online in May.
- * Brokers depend on the software to trade through modem links from their offices.
- * The trading floor is supposed to be closed permanently by 21 March.
- * Consequences of the breakdowns include lost commissions, lost business opportunities, and loss of confidence in the ASE.
- * EFA Software Services of Calgary responsible for trading software for other exchanges around the world, including the Palestine Securities Exchange.

I personally called EFA public relations and left a message requesting further details. More if and when I receive them.

Mich: M. E. Kabay, PhD, CISSP (Kirkland, QC), Director of Education
National Computer Security Association (Carlisle, PA) <http://www.ncsa.com>

⚡ Hot and cold running randomness

Dan Wing <dwing@Cisco.COM>

Mon, 10 Mar 1997 13:10:36 -0800

TBTF's 9 Mar 1997 issue carried this item:

#..Hot and cold running randomness

#

Perhaps for the first time, anyone with an Internet connection can

tap a source of true randomness. The creator of HotBits [16], John

Walker <kelvin@fourmilab.ch>, describes it as

#

> an Internet resource that brings genuine random numbers,

> generated by a process fundamentally governed by the inherent

> uncertainty in the quantum mechanical laws of nature, directly

> to your computer... HotBits are generated by timing successive

> pairs of radioactive decays... You order up your serving of

> HotBits by filling out a [Web] request form... the HotBits

> server flashes the random bytes back to you over the Web.

#

Walker modified an off-the-shelf radiation detector to interface to

a PC-compatible serial port, and ran a cable three floors down from

his office to a converted 70,000-litre subterranean water cistern

with metre-thick concrete walls, where the detector nestles with a

60-microcurie Krypton-85 radiation source.

#

If you're in the mood for an anti-Microsoft rant of uncommon eloquence,

Walker can supply that too [17].

```
#  
# Thanks to Keith Bostic <bostic@bostic.com> for the word on  
this  
# delightful service.  
#  
# [16] <URL:http://www.fourmilab.ch/hotbits/>  
# [17] <URL:http://www.fourmilab.ch/hotbits/source/hotbits-c.html>
```

An interesting idea, but hopefully no will use it -- it is too easily spoofed via DNS, and the host itself could be hacked to return the same 'random' number all the time. (Maybe after we have IPsec, SecDNS, _and_ you trust the host we could use services like this on the Internet).

Dan Wing dwing@cisco.com

🔥 Vietnam will censor Internet content

David Farber <farber@cis.upenn.edu>

Wed, 12 Mar 1997 06:15:30 -0500

All information coming into Vietnam through the Internet will be censored.

The Vietnamese government announced on 11 Mar 1997 that it will control who has access to online services. It also will limit the gates through which Internet servers in Vietnam are linked to the Internet.

A senior official at the General Department of Post and Telecommunications told Reuters the measures will take effect this month, but added they are still working on details and planned to meet in two months time to discuss implementation. The controls were issued in a decree by Prime

Minister Vo Van Kiet, who said information servers must be based in Vietnam. This will ensure that information entering and leaving Vietnam goes through a government-filtered gateway, the Communist Party newspaper, The People, reported.

[To our Vietnamese subscribers, please try to let us know if you ever fail to receive any particular issues of RISKS -- or if your subscriptions seem to have vanished. PGN]

✦ More RISKS-relevant ACM awards (Re: [RISKS-18.87](#))

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

Fri, 7 Mar 97 7:46:21 PST

Having mentioned in [RISKS-18.87](#) that the Kanellakis award was given to six crypto luminaries at ACM '97, I might as well note that two other ACM '97 awards also have RISKS relevance.

* Amir Pnueli is the recipient of the A.M. Turing Award, for his ``seminal work introducing temporal logic into computing science and for outstanding contributions to program and system verification.'' This work has been characterized as ``the most important contribution to program verification in the last 20 years.'' He is at the Weizmann Institute of Science in Israel.

* Peter J. Denning is the winner of the Karl V. Karlstrom Award, cited for his core-curriculum work and for communicating the intellectual

substance of computer science to other scientists and engineers. Peter has long been concerned with the role of fostering responsible and ethical behavior within the core curriculum. Denning has just become Vice Provost for Continuing Professional Education at George Mason University. (He was previously Chair of the Computer Science Department, and for a few more months will still be Associate Dean for computing.) The award cited his long standing efforts to shape our field and convey its nature to computer scientists and to the broader scientific community, and noted that his vision, leadership and early writings on operating systems played a key role in making that area a respected part of the core curriculum. He is a charter RISKS contributor, going back to volume 1 number 1.

✶ The Ariane 5 explosion: a software engineer's view

"Robert L. Baber" <bob@cs.wits.ac.za>

Tue, 11 Mar 1997 11:43:38 +0200

[Relevant to formal methods (e.g., the preceding item in this issue

on Amir Pnueli) and RISKS, Robert Baber's message is timely. PGN]

My web page "The Ariane 5 explosion as seen by a software engineer"

<http://www.cs.wits.ac.za/~bob/ariane5.htm>

shows how the software anomaly that caused the destruction of the Ariane 5

and its payload (a DM 1200 million loss) could have been avoided

by a simple application of correctness-proof techniques. It also highlights the importance of strict preconditions and the inadequacy of ordinary preconditions for practical applications.

Prof. Robert L. Baber, Computer Science Dept, University of the Witwatersrand
Johannesburg, 2050 Wits, South Africa +27-11-716-3794 bob@cs.wits.ac.za

✂ Usability and Security re: Authenticode (Atkinson, [RISKS-18.85](#))

Mary Ellen Zurko <zurko@opengroup.org>

Wed, 12 Mar 1997 12:55:08 -0500

In Bob's useful and interesting explication of Authenticode's design goals he states:

> IMHO, the most important innovations of Authenticode on prior general
> practice in the industry lie in the area of usability, especially as related
> to the user's understanding of and administration of trust.

He goes on to discuss this paradigm and some UI details.

However,

compelling and logical explanations of how usable some software is or will

be don't make it so. If intelligent engineers arguing about usability

produced it, we would have solved the problem years ago :-).

It's a good

start (always better to consider the user than not), but there are a bunch

of techniques for designing and testing software and other interfaces for

its usability. Those approaches do not guarantee usability (see the

previous comment on being solved), but they do get us closer and provide more compelling evidence of the claim, just as with performance evaluation requires tests to prove the results of a promised innovation. I would expect safety-critical systems to use these techniques regularly. So, since usable security is of particular interest to me, I'd like very much to hear about what design techniques and user testing were used to produce and verify this innovation in understanding trust. I know Microsoft has both the resources and the expertise to run these tests.

Mez

✶ CaptiveX/Authenticode

Henry G. Baker <hbaker@netcom.com>

Sat, 8 Mar 1997 08:31:58 -0800 (PST)

A major risk I have seen with respect to CaptiveX/Authenticode discussions is the effect it is having on unsophisticated users. These discussions happen not only among sophisticated people on comp.risks, but in the New York Times, the Wall Street Journal, MSNBC, CNN, etc.

In my not-very-scientific survey of people that I talk to, most people don't expect perfection from software, and therefore aren't very surprised, much less particularly outraged, by problems in CaptiveX. They appreciate the information about the problems, make notes to themselves to check with www.microsoft.com to get the fix, and go on with their lives.

We thus have the following situation: the 'man-on-the-street' thinks that CaptiveX is actually more secure/reliable than Java, because 'more of the bugs have been found & fixed'. In other words, your average bloke does not respond to news of CaptiveX problems by using Java. I.e., all of the clever thinking by Java people is wasted, since the customer doesn't appreciate it.

In fact, all of the discussions of IE problems is just more free publicity for Microsoft.

Here in La-La land, we've known for nearly a century that 'the only bad publicity is an obituary'. Thus, if companies are to be 'punished' for bad products, a more sophisticated approach will be required than the present hand-wringing.

Henry Baker <ftp://ftp.netcom.com/pub/hb/hbaker/home.html>

✶ Continual Risk/Benefit Analysis (Re: McCurley, [RISKS-18.86](#))

Benedikt Stockebrand <benedikt@devnull.ruhr.de>
09 Mar 1997 16:07:41 +0100

I quite agree that it is essential to understand the risk involved with actions to be taken. However, I consider the assumption of a "continual risk/benefit analysis" to be far too optimistic --- it falls for the well-known risk of assuming that people always behave rationally.

How many real world people don't fasten their seat belts while driving,
smash their thumb with a hammer too large for the job or trip over their
shoe laces they didn't bother to retighten? How many companies connect to
the Internet without a firewall? How many IE users have their IE security
level lowered to "medium" (which should rather be called "next-to-none"
anyway) or even below? How many people will happily allow an ActiveX applet
in if it promises some interactive video thing showing something sufficiently naughty?

Too many people will only perform the "risk/benefit analysis" *after*
they got bitten.

Of course, everybody is free to decide and subsequently has to live with the
consequences of the decisions made. But any responsible designer will take
this effect into consideration. And of course s/he will try to minimize the
risk/benefit ratio or even abandon a project if the risk can't be lowered to
an acceptable point.

Luring people into buying and using an unnecessarily insecure system and
telling them "to be careful" is plain irresponsible. Selling a super-fast
extra-shiny car without seat belts is negligent no matter if the manual
tells you not to drive without making sure you won't get involved in an
accident.

Benedikt Stockebrand, Dortmund, Germany

⚡ Re: Trusting the software vendor (Welsh, [RISKS-18.88](#))

David Collier-Brown <davecb@Canada.Sun.COM>

Mon, 10 Mar 1997 09:52:30 -0500

> ... Although with the advent of Java we are starting to
> see these ideas in the mainstream, they're not particularly
new.

Indeed, they're rather old, says the Multician(:-))

However, both the ActiveX and Java communities can improve on
the situation
considerably, by picking up some of the old, good ideas and
applying them to
current technology.

If I want to run a semi-trusted program with access to a chunk
of my disk
space, I can say so with only a small extension to currently-
available ACLs
(Access Control Lists, available on many Unix variants and
Windows NT).

Assume that I have the ability to define a specific instance of
myself, and
give it a name visible to the ACL processor. Call the instance
'browser'

Then I can say

```
/home/davecb/catbox rw davecb.browser
```

and run a Java applet or ActiveX control and let it access the
catbox.

Let's expand on this a bit: add a list of authenticode
signatures and a
notation for representing them in the ACL file, and I can say

```
/home/davecb/fred w davecb.signed(fred)
```


in order to allow an applet signed by fred to write to /home/
davecb/fred.

Alas, this doesn't come without risks of its own. If there is
no mandatory

access control ("MAC") mechanism, I can allow untrusted controls to access anything I have access to... just by writing a bad acl rule. Even worse, I might write a rule that allows anyone else who has write access to my files to run any applet whatsoever with write access to my files.

The risk here is a classical one: there are lots of ways to achieve access control, and many of them are ill-considered. A reading of the literature on MAC and ambiguous interfaces is highly desirable before looking into ways of giving more access to arbitrary programs. (Darn!)

David Collier-Brown, 185 Ellerslie Ave., Willowdale, Ontario N2M 1Y3 CANADA
1-416-223-8968 davecb@hobbes.ss.org, <http://java.science.yorku.ca/~davecb>

✦ Re: Trusting the software vendor (Welsh, [RISKS-18.88](#))

Daniel Hicks <hotlicks@VNET.IBM.COM>
Mon, 10 Mar 1997 10:27:27 -0600 (CST)

Having been associated with the IBM S/38 & AS/400 for twenty years, I have to agree with Mr. Welsh. The AS/400 uses a "trusted translator" which is conceptually very similar to the Java trusted verifier/interpreter approach. Years of experience have shown that this technique can be used to maintain integrity in a system without the need for elaborate hardware protection, while at the same time giving programmers relatively free rein to produce the sort of code they want.

I have had the opportunity to examine the Java JVM spec in considerable detail, and, based on my experience with similar concepts in the AS/400, it appears to be sound. Similarly, the security manager scheme appears sound, though I haven't examined it in as much detail.

As always, there is ample opportunity for bugs, both in the specs and in the implementations, but it seems wise to at least BEGIN with the concept of a secure system and then fix the bugs, rather than begin with a hopelessly insecure system and struggle to make it secure.

Re Wayne Gerdes' complaints about the limitations of the Java Applet environment, these are of a transient nature. It seems clear that the Applet environment can be augmented to provide more capabilities, but, unlike ActiveX, this can be done in a fine-grained incremental fashion as experience brings to light both the need for and the hazards of these additional capabilities.

Dan Hicks

✶ **ActiveX Security for Dummies (Re: [RISKS-18.85-86](#))**

Peter Gutmann <pgut001@cs.auckland.ac.nz>

Wed, 12 Mar 1997 06:12:48 (NZDT)

The recent messages on ActiveX/Authenticode security have prompted me to submit the following simple description of Authenticode security and why it

doesn't work. It's very non-technical, and doesn't require any knowledge of digital signatures or anything similar. It's been tested on the local ActiveX glee club, and seems to work:

Imagine a large, security-conscious office building. At the main entrance is a security desk where anyone entering the building is required to present some form of ID like a drivers license, and sign in. If you don't have your ID, the security guards have the option of turning you away. Once you've signed in for the first time, you're allowed free run of the building. You can take anything you want into and out of the building and roam the building at will, as long as you flash your drivers license at the security guard noone ever checks anything else.

One day a huge explosion rocks the building, destroying most of it and killing a great many people. There is no evidence left after the explosion which can be used to find out exactly what happened.

Scenario 1 (less likely):

The security guards have logs of everyone who entered, a total of nearly 3000 people in the last few months (remember that there is *no* other evidence). How are these logs going to help pinpoint who caused the explosion?

Scenario 2 (more likely):

The logs were destroyed during the explosion along with everything else.

How do you find out who caused the explosion?

I think the parallels with ActiveX and Authenticode are obvious.

Peter

⚡ The real goal of Authenticode

Mark Seecof <Mark.Seecof@latimes.com>

Tue, 11 Mar 1997 22:24:01 -0800

In [RISKS-18.85](#) Bob Atkinson gave us quite a bit of insight into the thinking behind the design of MS-Authenticode. In [RISKS-18.86](#) a number of experts analyzed and/or criticized Authenticode from a technical point of view. While I learned quite a bit from both issues of RISKS, I think one very important factor which may have motivated Microsoft to ship Authenticode was not aired.

I suspect that Authenticode may serve as a competitive weapon for Microsoft in ways which MS has not chosen to discuss. Below I will suggest a simple observational test for my hypothesis.

As all experts have pointed out, Authenticode does not even try to protect the end-user from malicious code. All it can do is identify the source of some code with a degree of reliability heretofore unavailable (I ignore any question of bugs in Authenticode as implemented).

Now, Microsoft does not, generally speaking, purvey malicious code. Sure, it ships a lot of bugs and occasionally a virus, but MS is

basically trustworthy. Certainly all the users of Windoze and MS-* trust MS, and that's perfectly reasonable. For this reason, users who download code signed *by Microsoft* can use it with reasonable confidence.

Users will have less confidence in code signed by others. Even if those others are well-known and trusted vendors (e.g., Borland), users may not be able to verify their signatures. Authenticode ships with verification for MS' signatures.

Imagine the user who calls (at MS' per-incident rate of \$95 paid in advance)

for help: "Windows bombs every time I press the START button!"

"Have you been exploring(tm) the Internet?" "Yes. For weeks."

"Did you run any software from the Internet?" "Yes. Lots."

"Was it all signed by Microsoft?" "No."

"Well, I'm afraid you'll have to call the vendors who supplied any software you got from the Internet. If they can't help you, though, you should try reinstalling Windows. Good luck! [Click.]"

See, it doesn't matter who signed the software if it wasn't Microsoft. Your warranty is void.

Therefore it does not matter if Authenticode helps anyone to avoid malware from arbitrary suppliers or not (the technical reasons why it won't have already been aired).

MS states clearly (and Atkinson confirms) that MS expects end-users to take

responsibility for bad results--since they "trusted" someone they oughtn't have. This is a good position for Microsoft, which refuses categorically to improve the security and stability of its OS software (or even to document it thoroughly--some people think this is so that competitors in the application arena will have more trouble shipping compatible software). Why should MS take bad press for OS holes when it can blame everything on careless users?

Authenticode exists chiefly to authenticate *Microsoft software* and thereby aid Microsoft marketing. Whenever Authenticode pops up to warn a user that he is about to risk trashing his PC by installing something that (gasp) is *not from Microsoft* that user gets a little stab in the psyche: code which is *not from Microsoft* is *dangerous*.

Now, I did promise a test. If MS announces any sort of co-branding or other arrangement under which, for a fee (or for early product intelligence), MS will sign *other people's* code, you will know that my hypothesis is correct. (It might be correct anyway; I'm just offering one possible test.) I would regard any offer by Microsoft to validate signatures from other vendors through MS' networks as suggestive though not conclusive proof--MS could get only smaller fees and less valuable intelligence from such a service, and offering it would reduce their marketing benefits.

Mark Seecof

[I have selected just a few recent representative

contributions on
this topic, in the hopes of not overwhelming our readers. PGN]

✶ CFP: DIMACS Workshop on Formal Verification of Security Protocols

Catherine A. Meadows <meadows@itd.nrl.navy.mil>

Wed, 12 Mar 1997 15:37:12 -0500 (EST)

DIMACS Workshop on Formal Verification of Security Protocols, 3-5 Sep 1997

Organizers: Hilarie Orman, DARPA and Catherine Meadows, Naval Research Lab.

As we come to rely more and more upon computer networks to perform vital functions, the need for cryptographic protocols that can enforce a variety of security properties has become more and more important. Thus it is no surprise that in recent years a number of new protocols have been proposed for such applications as electronic credit card transactions, Web browsing, and so forth. Since it is notoriously difficult to design cryptographic protocols correctly, this increased reliance on them to provide security has become cause for some concern. This is especially the case since many of the new protocols are extremely complex.

In answer to these needs, research has been intensifying in the application of formal methods to cryptographic protocol verification. Recently this work has matured enough so that it is starting to see application to real-life protocols. The goal of this workshop is to facilitate

this

process by bringing together those who are involved in the design and standardization of cryptographic protocols, and those who are developing and using formal methods techniques for the verification of such protocols. To this end we plan to alternate papers with panels soliciting new paths for research. We are particularly interested in paper and panel proposals addressing new protocols with respect to their formal and informal analysis.

Other topics of interest include, but are not limited to

- Progress in belief logics
- Use of theorem provers and model checkers in verifying crypto protocols
- Interaction between protocols and cryptographic modes of operation
- Methods for unifying documentation and formal, verifiable specification
- Methods for incorporating formal methods into crypto protocol design
- Verification of cryptographic API systems
- Formal definition of correctness of a cryptographic protocol
- Arithmetic capability required for proofs of security for number-theoretic systems
- Formal definitions of cryptographic protocol requirements
- Design methodologies
- Emerging needs and new uses for cryptographic protocols
- Multiparty protocols, in particular design and verification methods

We encourage attendees to bring tools for demonstration.

Information about

availability of facilities for demonstration will be posted later.

To submit a paper to the workshop, submit a one or two page abstract, in

Postscript or ASCII to both organizers at the e-mail addresses

given below by
June 16, 1997. Authors will be notified of acceptance or
rejection of
abstracts by July 1. Full papers will be due by August 1.
Copies of papers
will be distributed at the workshop. We also plan to publish a
proceedings.

Participation in the workshop is **not** limited to those giving
presentations.

If you would like to attend the workshop, a registration form is
available
at http://dimacs.rutgers.edu/Workshops/Cryptographic/reg_form.html.

Information on accommodations and travel arrangements is
available at
<http://dimacs.rutgers.edu/Workshops/general/accommodations.html>
and
<http://dimacs.rutgers.edu/Workshops/general/travel.html>.

Information on the workshop in general is at
<http://dimacs.rutgers.edu/Workshops/Cryptographic>.

Organizers

Hilarie Orman
DARPA ITO
3701 N. Fairfax Drive
Arlington VA 22203-1714
phone: (703)696-2234
e-mail: horman@darpa.mil

Catherine Meadows
Naval Research Laboratory
Code 5543
Washington, DC 20375
phone: (202)-767-3490
e-mail: meadows@itd.nrl.navy.mil



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 18: Issue 90

Friday 14 March 1997

Contents

- [Trojan-horsing around with video tapes](#)
[John Janieri via PGN](#)
- [Swedish Cracker Disrupts Florida 911 Systems](#)
[Edupage](#)
- [AOL Says It Got Incorrect Stock Info From S&P](#)
[Edupage](#)
- [News from the Land of Tamperproof Things](#)
[Peter Wayner](#)
- [NCAA Gives FBI Info on Web Site Vandalism](#)
[Edupage](#)
- [Dorothy Denning key-escrow/policy paper on-line](#)
[Mark Seecof](#)
[Dorothy Denning](#)
- [Hardening Your Computing Assets: Defending Against HERF and EMP](#)
[Carlo Kopp via Winn Schwartau](#)
- [Risks associated with upgrading to MS Office 97](#)
[Lloyd Wood](#)
- [Re: CaptiveX/Authenticode](#)
[Mark Bergman](#)
- [Risks of random-number server](#)

[Dan Drake](#)

● [Telephone Scam](#)

[Dewi Daniels](#)

● [Re: Not dead yet -- I'm still 3 degrees!](#)

[David Fetrow](#)

● [Re: The Ariane 5 explosion: software engineer's view](#)

[Kevin F. Quinn](#)

● [Keith Rhodes: Y2K duns contractor for 97-year delinquency](#)

[Robin Sheppard](#)

● [Y2K: the revenge of originality](#)

[Peter Vaneynde](#)

● [Y2K & UNIX & Netscape, the end is HERE](#)

[Geoffrey Cooper](#)

● [Y2K "problem" in virus?](#)

[Dean Matsen](#)

● [InfoWarCon 7: Call for Papers](#)

[Betty G. O'Hearn](#)

● [Info on RISKS \(comp.risks\)](#)

⚡ Trojan-horsing around with video tapes

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

Thu, 13 Mar 1997 11:21:45 PST

John V.A. Janieri in the Software Safety Research Group at Underwriters Laboratories in Research Triangle Park NC sent me a copy of a letter

(undated, but received on 25 Jan 1997) that he received from Gateway 2000.

The RISKS-relevant excerpt is this:

Dear Gateway Customer: We are recalling our promotional video tapes

made between December 20, 1996, and January 6, 1997. It appears

that an individual employed by an outside supplier to Gateway

tampered

with some of our video tapes and inserted offensive and objectionable

material. Enclosed is your new Gateway 2000 video tape. The shrink

wrapping on the new tape is your assurance that it is an official

Gateway product. It is also our guarantee that we have protected you

and your family from the problem we've recently experienced. [...]

Dr. James Allen Taylor, Senior Vice President, Gateway 2000

I suppose John's association with UL is particularly appropriate in this

case, because the spoofed tapes in question had not only a writer, but an

under-writer (à la sous-chef). On the other hand, I imagine that UL

would not underwrite the strength of the ``guarantees'' mentioned by

Dr. Taylor.

Swedish Cracker Disrupts Florida 911 Systems (Edupage)

Edupage Editors <educom@elanor.oit.unc.edu>

Sun, 9 Mar 1997 18:53:44 -0500

A Swedish computer cracker was able to dial into 11 north Florida 911

systems, tying up lines and harassing operators, the FBI reported Friday.

"In a few of them it was just a one-time incident where he would hook up a

911 operator with another 911 operator. In other jurisdictions it was

multiple times," says an FBI agent. The man has been arrested and convicted

of a misdemeanor in Sweden, because it has no laws that address electronic

intrusion. (*Tampa Tribune*, 8 Mar 1997; Edupage, 9 March 1997)

⚡ AOL Says It Got Incorrect Stock Info From S&P (Edupage)

Edupage Editors <educom@elanor.oit.unc.edu>

Sun, 9 Mar 1997 18:53:44 -0500

While acknowledging that it posted some inaccurate information about Ben

Ezra Weinstein & Co., America Online blamed the problem on bad information

it had received from Standard & Poor, its stock information supplier. An

AOL spokesperson says: "We don't make the stock prices. All the information

is computer-translated, and occasionally the information we get is wrong."

But the chief operating officer for Ben Ezra Weinstein suggests otherwise:

"AOL just acknowledged that they've known about the problem for a few weeks

but couldn't correct it until they got a certain software. When I asked AOL

to put that in writing, they wouldn't... We believe the problem is with

AOL, and we have asked them to fix the problem and provide a screen saying

there been errors, and they haven't done either." (*Atlanta Journal-Constitution*, 7 Mar 1997; Edupage, 9 March 1997)

⚡ News from the Land of Tamperproof Things

Peter Wayner <pcw@access.digex.net>

Thu, 13 Mar 1997 16:12:57 -0500 (EST)

The *Wall Street Journal* (13 Mar 1997) reports that Roger

Johnston, Los Alamos employee, ``prides himself on being able to open anything-- and without leaving a trace.'' The article continues to describe how he opens sealed boxes, cargo bins, and shipping containers with ordinary dentist and locksmith tools. He prides himself on not leaving any evidence of his attack. Although the article doesn't directly address tamperproof smart cards popular in digital cash circles, it quotes Mr. Johnson as saying, ``We haven't found anything that we can't defeat.''

⚡ NCAA Gives FBI Info on Web Site Vandalism (Edupage)

Edupage Editors <educom@elanor.oit.unc.edu>

Thu, 13 Mar 1997 14:03:55 -0500

The National Collegiate Athletic Association (NCAA), victimized by a vandal who cracked into the NCAA's Web site to post racial slurs there, is turning over to the FBI all details of the malicious entry. The Kansas City Star says it has identified the vandal as a 14-year-old high school freshman. (AP, 12 Mar 1997; Edupage, 13 March 1997)

⚡ Dorothy Denning key-escrow/policy paper on-line

Mark Seecof <Mark.Seecof@latimes.com>

Thu, 13 Mar 1997 20:42:04 -0800

A recent paper presented by Dorothy Denning to the "Australian/

OECD

Conference on Security, Privacy, etc. in the Global Information Infrastructure" advocating key-escrow encryption and the criminalization of secure cryptography is available at <<http://www.nla.gov.au/gii/dd.html>>. I

recommend this paper to those interested in security policy issues.

The most important feature of the paper is Denning's refusal to recognize the possibility of misconduct or incompetence by escrowed-key holders or the governments to which they may be subject. She does not even mention these threats to dismiss them.

Dr. Denning expends a surprising number of words on the evils of "crypto-anarchists," a group she defines (partly by omitting to mention any middle-grounders) as all who disagree with her notions of proper (in-)security methods. She actually tars the IETF IP Security Working Group with this brush.

Denning advocates restrictive licensing for the manufacture and use of security software. She does not mention any conflict between her proposals and either the U.S.' 1st Amendment or various international human-rights conventions.

While Denning cites and discusses remarks from a number of political sources, and some technical ones with respect to key-escrow systems, she does not cite any "uncongenial" technical sources (like, say, Matt Blaze) nor discuss any work which might provoke anyone to question her conclusions.

Lastly, though she describes how info security may often be

compromised
without breaking any ciphers (by, say, obtaining physical access
to
computers) she also suggests that effective encryption would
completely
stymie police agencies. I beg to suggest that (a) effective
encryption
would hardly leave police with fewer investigative means than
they had
before people commonly had computers, and (b) police are much
more able to
use non-cryptanalytic means to obtain information than, say,
hackers. For
example, encrypted digital telephones might baffle hackers and
police alike,
but police could and would simply bug the rooms containing the
'phones to
obtain the conversations. (Since Denning cites Russia for its
crypto-licensing policy, I should cite it for the ultimate
investigative
tool--questioning suspects under torture--which I was surprised
to see
Denning did **not** count as a bad result of good encryption.
Maybe she will
next time, little as I care to assist her.)

Mark Seecof

✶ Dorothy Denning key-escrow/policy paper on-line

Dorothy Denning <denning@cs.georgetown.edu>
Fri, 14 Mar 1997 16:28:52 -0500

The "recent" paper that Mark Seecof refers to is over a year old
(even that
was a revision of a paper now 2 years old!). It does not
reflect my current
thinking, and I too find much to criticize in it. Readers
interested in my

recent thinking (which is constantly undergoing revision!) should read my latest paper "Encryption Policy and Market Trends". All of the papers mentioned here are available at <http://www.cs.georgetown.edu/~denning/crypto/> .

Mr. Seecof has read much between the lines of my paper that are not supported by facts. Even though I did not write about it in the paper, I do recognize the potential for misconduct or incompetence on the part of key escrow agents or governments. It was one reason why I signed up to review the government's Clipper system in 1993. I wanted to help make sure that that system had extremely good safeguards. Some of my other papers say more on this topic. For example, the following is from "Encrypting the Global Information Infrastructure," Aug. 19, 1996:

"Large-scale deployment of key escrow introduces some risk into the infrastructure. Key escrow is not likely to be accepted unless users are convinced that these risks have been made negligible through technical, legal, and procedural safeguards, and that they will be able to recover losses in case of abuse. Users will want to be able to pick key holders they trust. They will want assurances that key escrow will not be exploited by corrupt governments to violate human rights and that government-to-government agreements will not make them vulnerable to foreign espionage."

In that paper I was not advocating mandatory key escrow. In the paper Seecof refers to, I did discuss the possibility of such controls

on the
manufacture and distribution (but not use) of encryption
products. I
believe it is important that we openly discuss a variety of
options.
However, I have not advocated mandatory key escrow. I do
advocate the
use of strong cryptography, and I advocate key recovery systems
as good
business policy.

I did not mean to suggest that people who disagree with me are
evil or that
cryptoanarchists are evil. It was particularly unfortunate that
my mention
of the IETF was interpreted to mean that I viewed them as either
cryptoanarchists or evil. I have considerable respect for many
of the
people who work on the standards, and I support the standards
they have
developed. The crypto in IPv6 is a good thing!

I have written about export controls on encryption software and
1st
Amendment issues. See "Export Controls, Encryption Software,
and Speech."
See also "Is Encryption Speech?"

Yes, I could have cited more sources than I did and said more
than I said.
By all means, read the works by Matt Blaze and others.

I am currently in the middle of a more comprehensive study of
the impact of
crypto on crime and terrorism. Input welcome, especially from
people with
actual case experience. Stay tuned.

Dorothy Denning

✦ Hardening Your Computing Assets: Defending Against HERF and EMP

by way of "Betty G. O'Hearn" <betty@infowar.com> <winn@infowar.com>

Wed, 12 Mar 1997 13:59:31 -0500

The Subject: line is the title of another excellent paper by Mr. Carlo Kopp, a noted defence analyst and aviation writer from Australia. This is a HERF Guns and Magnetic Weapons update. The paper is very understandable with methods for protecting computer systems and networks from externally induced power events that can cause havoc with electronic systems and controls.

Mr. Kopp provides excellent graphics to further illustrate his recommendations on Defending IW, Site Hardening, and Hardening Computer Equipment. For extreme denial of service attacks and terrorist worries, this is a fine example of creative thinking and defensive posture.

Kopp states, "Indeed, the commercial opportunities for smaller manufacturers in the production of hardened equipment chassis and interfaces, using standard commercial internals, are considerable in the medium term. We can hope that our industry will rise to this challenge."

I highly recommend this well written and informative piece. It is available at no charge on www.infowar.com, at URL:

http://www.infowar.com/class_3/harden.html-ssi

Winn Schwartau www.infowar.com www.info-sec.com

✦ Risks associated with upgrading to MS Office 97

Lloyd Wood <L.Wood@surrey.ac.uk>

Thu, 13 Mar 1997 16:29:30 +0000 (GMT)

This was a university-wide advice memo received today.

It illustrates some of the risks of relying on a product with a publically undocumented proprietary data format with an all-new internal format; you have to wait for third-parties to get the information they need, and provide essential support for problems that shouldn't exist in the first place -- like recovery of files damaged, perhaps by Office macro viruses.

<URL:<http://www.sat-net.com/L.Wood/>><L.Wood@ieee.org>+44-1483-300800x3435

[and I want 'open standards' tattooed on my forehead.]

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

Date: Thu, 13 Mar 1997 12:43:23 +0000

>From: XXX

To: XXX

Subject: Risks associated with upgrading to MS Office 97

*****Use caution when upgrading to Microsoft Office 97*****

The Microsoft Office 97 suite uses different file formats to that used in the earlier version. This means that earlier virus protection products will not afford the level of protection all user require and expect from their previously installed anti-virus software.

Microsoft have acknowledged the fact that in the rush to market the product, they did not release the information regarding this change of file format to anti-virus vendors in time for them to prepare their products.

In any event, the University's site licensed anti-virus product, McAfee VirusScan 2.5.x DOES NOT afford Office 97 users an adequate level of protection. This version, and earlier versions of McAfee have been available from the UCS Service Desk for some time.

McAfee recently launched (March 3, 1997) VirusScan 3.0 with the Hunter(tm) Virus Detection Engine that includes Office 97 Macro virus protection and it successfully detected 100% of viruses in the latest Secure Computing Magazine review (McAfee's statement-for details of the tests please consult the magazine as this reported success rate does depend on the test conditions). UCS are awaiting the arrival of this latest version.

Whilst this article refers to McAfee anti-virus products, you must check with other vendors such as Symantec and Dr Solomon for up to date news if you use their products.

[sig snipped. UCS = University Computing Services]

✉ Re: CaptiveX/Authenticode (Baker [RISKS-18.89](#))

Mark Bergman <bergman@panix.com>

14 Mar 1997 15:20:27 -0500

I think the perception issues are more serious than [Henry Baker states]. I was recently part of a planning meeting where a strategic shift from Apple to Wintel platforms was discussed. One of the arguments in

favor of Windows

95 (from a senior molecular-biochemist) was that "Apple keeps releasing all these patches and bug fixes and upgrades to their operating system, while Microsoft hasn't released anything for Windows95" as evidence that Win95 is therefore bug-free.

The RISK? Things are worst when they appear best. Even smart people don't always get it.

Mark Bergman Biker, IATSE #1 Stagehand, Unix mechanic
718-855-9148 bergman@panix.com {cmcl2,uunet}!panix!bergman

✂ Risks of random-number server (Re: Wing, [RISKS-18.89](#))

Dan Drake <drake@A.crl.com>

Thu, 13 Mar 97 09:42:55 -0800

First, a bias disclosure: as a friend of the provider of the service described here, I'm more annoyed by this carping than other people might be. Now then,

[Description of quantum-based random-number server at <http://www.fourmilab.ch/hotbits/>, followed by] >

> An interesting idea, but hopefully nobody will use it -- it is too easily
> spoofed via DNS, and the host itself could be hacked to return the same
> 'random' number all the time. ...

What, nobody? How about people who know who's providing the service, and can make a reasonable comparison between the hacking probability

at his
site versus that at other sites, like the Department of Defense?

How about people with the sense to run occasional spot checks on
the
output to see if it looks reasonably random?

Of course, the guys in the black helicopters could pollute the
data, via DNS
spoofing or whatever, only occasionally, and instead of
returning the same
number all the time, they could replace these quantum random
numbers with
output from some Microsoft random() function to circumvent the
spot checks.

The Risks question here is, just what level of paranoia is
suitable here?

The real risk here is that this may annoy John enough that he'll
waste his
valuable time adding a PGP signature capability to the random-
number output.

Spoof that.

Dan Drake dandrake@netcom.com [http://www.nbn.com/people/
dandrake/index.html](http://www.nbn.com/people/dandrake/index.html)

Telephone Scam

Dewi Daniels <dewi@cableol.co.uk>

Fri, 14 Mar 1997 12:07:26 GMT

We had a nasty shock a couple of days ago, when we received our
monthly
phone bill from our cable telephone operator, CableTel. The last
two days of
the billing period, there had been a number of calls to the same

number in

Guyana, totalling UKP 75, more than doubling our phone bill. On each day, there had been three calls in succession, making a total of six calls.

We placed a bar on premium rate and international calls as soon as we received the bill. I'm concerned these calls may have continued to be made during the week that elapsed before we received the bill, so we could be liable for another UKP 250 or more.

We got in touch with CableTel, who claim that these calls had originated as premium rate calls to an 'entertainment' line, and that their records showed these calls must have been made from our house.

Now, we're sure that nobody made these calls from our house. I was in the USA at the time, and my wife was at work. A married couple, old friends of ours, were staying with us. At the time of the calls, the husband was at home, studying for his Open University degree, and the wife was at work. We had no workmen or other visitors in the house those days.

It's not clear yet whether CableTel are going to hold us liable for these charges. It is clear that they suspect our friends. I can't say I blame them for coming to that conclusion, but we have every reason to believe that our friends are perfectly trustworthy, and are sure that the explanation must lie elsewhere.

As a software safety engineer, and a regular reader of the RISKS Digest, I'm well aware there may be any number of ways in which these calls

could have
been charged to our account. I find CableTel's claims that their
computer
records 'prove' the calls were made from our house to be rather
less than
satisfying.

I don't have any detailed knowledge of telephony or telephone
billing
systems. I do, however, respect the technical knowledge of my
fellow
subscribers to this list. Does anyone have any theories as to
how these
calls could have been charged to our account, or has anyone
heard of any
similar cases?

I'd be very grateful indeed for any suggestions as to how we
should
proceed in presenting our case to CableTel.

Dewi Daniels Guildford, England

[Please reply to Dewi, cc:ing RISKS. Dewi, please
summarize your answers for RISKS. TNX. PGN]

⚡ Re: Not dead yet -- I'm still 3 degrees! (Seurer, [RISKS-18.87](#))

David Fetrow <fetrow@biostat.washington.edu>
Fri, 14 Mar 1997 10:44:47 -0800 (PST)

> On a medical device with 4 digits output what sort of
meaningful error code
> would you expect? [...]

Although these are valid points and it's just a thermometer:

Hospital medical equipment must be utterly clear about what the
problem is

without consulting a manual (or even the bottom of the unit). If that means spending an extra \$2 for an alphanumeric display so be it.

Error codes such as a "3" are NOT OK. Even if it's "obvious when you think about it" this kind of error code means the caregiver is spending time diagnosing a box of electronics and not the patient.

Throw in a lack of standardization of what the codes mean, a need not to pick up random stuff with gloved hands, time constraints, temporary help, hooking people up to a dozen devices.... There hardly seems enough attention left to deal with a patient.

✶ Re: The Ariane 5 explosion: software engineer's view (Baber, R-18.89)

"Kevin F. Quinn" <kfq@wormhole.compd.com>

Fri, 14 Mar 1997 12:22:24 +0000

I think it is worth noting that there are many commonly-used engineering techniques that would have detected the fault during development, some of which are mentioned in the inquiry board's report as having been compromised.

Application of correctness-proof techniques as described by Professor Baker could no doubt have detected the failure, unfortunately such techniques require a facility in mathematics that is rare in software engineers (and in almost all other groups, for that matter). The potential for error in

application of such techniques surely has to be considered. Unquestionably when accurately applied the techniques could have avoided the problem, but how accurately would they be deployed in practice? The same is true of other engineering practices designed to avoid such failures; those in use on the Ariane 5 programme if rigorously applied would have detected the fault.

(The report mentions several cases where practices were deliberately compromised in this case; continued operation of the alignment function after lift-off - that function being meaningless after lift off on Ariane 5, lack of redundant software in the two SRIs, lack of closed-loop system testing including the SRIs, not designing flight-critical equipment as fail-operate where possible, and so on.)

The risk is to trust any particular engineering technique when so much else can compromise the system without compromising the technique as such itself (i.e. assuming that the technique is accurately applied). In this case, my understanding is that an assumption was made that the BH (horizontal bias) value would not exceed the expected range for the alignment function. The assumption possibly arising from only considering the alignment function in a pre-lift off situation, which given that the function is meaningless after lift-off would not be unreasonable. It is easy to conceive that in the same environment, formal methods of proof would be applied under the same assumptions, and hence could be compromised in the same fashion.

Kevin F. Quinn - Software Engineer kfq@wormhole.compd.com (work)
kevgq@banana.demon.co.uk (home) <http://www.banana.demon.co.uk/>

⚡ Keith Rhodes: Y2K duns contractor for 97-year delinquency

Robin Sheppard <robinsheppard@technologist.com>

Thu, 13 Mar 1997 07:43:24 -0800 (PST)

RISKS of things to come:

>From **The Napa Sentinel** (Napa, CA), March 7, 1997:

"In testimony last week before the House Government Reform Committee, Keith Rhodes of the Government Accounting Office described what happened when a three-year defense contract was awarded last month, for completion in January 2000. A computer read the date as 1900 (the last 2 digits), and sent the contractor a 97-year delinquency notice."

The writer opined that "It stands to reason. Before they could invent artificial intelligence, they had to come up with artificial dumbness."

Robin Sheppard robinsheppard@technologist.com

⚡ Y2K: the revenge of originality

"Peter.Vaneynde" <s950045@uia.ua.ac.be>

Mon, 24 Feb 1997 09:44:10 +0100 (MET)

A few days ago I had a conversation with an old friend who now works with a

subcontractor at one of the largest insurers in this country. He told me that he was working on the Y2K problem (in COBOL; I offered my condolences). I asked how many lines of code he could check in a day. I was quite surprised to learn that they only did a search for names that alluded to the involvement of dates (date|time|datum|tijd etc). Later I remembered an other conversation with a neighbor who works at an other insurer: he told me of a colleague who used nonsense words as identifiers (dada, pipi, woef, miauw, etc).

Exercise for the reader: what is the chance that similar "problem-solving" techniques touch code generated by "original" programmers? Man, now I'm scared about 2000.

⚡ Y2K & UNIX & Netscape, the end is HERE

Geoffrey Cooper <geof@devices.com>

Tue, 11 Mar 1997 14:30:02 -0800

Well, we added Y2K support for our new little Twister web server box, which has a PC-compatible time chip in it (yes, I know, but it was cheap). Then we found that Netscape 3.0 was crashing on certain files. One machine was initialized incorrectly, and was serving up file-modification times as the year 2050. Netscape appears to cache the file with a UNIX-compatible time stamp, and 2050 is a negative date.

We decided to retire the product in (or at least upgrade the flash ROM

by) the year 2037.

Geoffrey Cooper, Compact Devices, Inc., Campbell, CA 408 255
4200
geof@devices.com

⚡ Y2K "problem" in virus?

Dean Matsen <dmatsen@halcyon.com>
Sun, 23 Feb 1997 00:45:16 GMT

> Has anyone bothered to look and see if the Michaelangelo virus
will be
> bitten by the Y2K problem? One can only hope...

I have actually seen and disassembled the Michaelangelo virus
code. It
doesn't care what year it is, only that it's March 6th -- This
virus will be
a risk as long as it lives. Bummer.

⚡ InfoWarCon 7: Call for Papers

"Betty G. O'Hearn" <betty@infowar.com>
Fri, 14 Mar 1997 14:58:44 -0500

Defensive Information Warfare and Systems Assurance
For Community, Company and Country
Sheraton Premier, Tysons Corner, VA, September 11-12, 1997
Call for Papers

Sponsors: National Computer Security Association <<http://www.ncsa.com>>

and Winn Schwartau, Interpact, Inc. <<http://www.infowar.com>>
and <<http://www.info-sec.com>>

Submission Deadline: May 16, 1997

For complete information on attendance:

Registration: Conferences@ncsa.com

Sponsorships: Sponsors@ncsa.com

Questions/Help: betty@infowar.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 18: Issue 91

Monday 17 March 1997

Contents

- ["Grounding of the Royal Majesty"](#)
[John Berg in searoom-1 from Steve Schultz via Mike McLaughlin](#)
- [Risks of losing your identity](#)
[CALPIRG item from PGN](#)
- [Ignoring smart-card risks](#)
[David Randolph](#)
- [Shockwave security hole exposes e-mail](#)
[Sidney Markowitz](#)
- [Risks of online commerce](#)
[Paul O'Donnell](#)
- [Experiences with a Year-2000 credit card](#)
[Robert Bowdidge](#)
- [Re: Y2K: the revenge of originality](#)
[Amos Shapir](#)
- [Risks of random-number servers](#)
[Eric Rescorla](#)
- [Ariane 5 - a wry comment](#)
[C. Shen Orr](#)
- [Re: Telephone Scam](#)
[Lou Fernandez](#)

revenue, the
>incident cost U.S.\$7 million. The N.T.S.B. report said the crew
members were
>not adequately trained in the use of the automated capabilities
of the
>ship's integrated bridge system, including an STN ATLAS
Elektronik G.m.b.H.
>Navigation Command System (NACOS 25) with two input ports for a
Raytheon
>G.P.S. receiver and a Raytheon Loran C receiver. Crew members'
training was
>limited to on-the-job knowledge from each other, with no
performance or
>training standards, no inspections and no certifications. An
hour out of
>Bermuda, an antenna cable connection on a G.P.S. receiver was
severed. The
>system defaulted to dead reckoning when the cable was
disrupted, and did
>not account for wind or sea changes. The automated display
therefore showed
>the ship on course. The ship failed to acknowledge alarms,
visual warnings,
>aids to navigation including channel buoys and lights and
differences in
>water color. Norwegian Cruise Line recently announced plans to
buy the
>Royal Majesty from Kvaerner A.S.A. for U.S.\$190 million.
>[...]
> World Maritime News is distributed by electronic mail
every Friday.
>Due to its distribution beyond the original format both in
style and
>medium, it is preferred that it be left intact or that World
Maritime News
>and/or Steve Schultz (sschultz@execpc.com) be attached with
excerpts,
>especially those excerpts in which structure and tone are not
changed from
>that used in the World Maritime News. If in doubt, please ask.
Although
>every effort has been made to verify the accuracy of the
information

>presented, I do not assume any liability arising from its use.
>[...]
End of searoom-1 V1 #394

⚡ Risks of losing your identity

"Peter G. Neumann" <neumann@csl.sri.com>
Mon, 17 Mar 97 10:02:14 PST

CALPIRG (a public-interest research group) has a new Theft Identity Guide ('`What Can Consumers Do To Avoid Becoming Theft-of-Identity Victims?') for any of you who want to know what you can do to protect yourself against having your identity misappropriated. I worked my way down the PIRG Website and found the Guide at <http://www.pirg.org/calpirg/consumer/privacy/toi/prevent.htm> . If you cannot get a Web copy, send e-mail to watchdog@pirg.org, or call 1-800-533-4449 within the U.S., or write to CALPIRG at 11965 Venice Blvd #408, Los Angeles 90066.

If you are a new RISKS reader and don't know about the potential risks, the RISKS archives contain a startling number of cases involving individuals whose identity has been usurped, purloined, lost, or otherwise impaired. Some of the early cases are summarized in my Inside Risks column, CACM, 35, 1, January 1992, and more recently in my RISKS book (Computer-Related Risks, Addison Wesley, 1995, pages 194-199). The RISKS archives include (among others) the following cases -- itemized in the Illustrative Risks summary

(<ftp://ftp.csl.sri.com/illustrative.PS>), with references (S i j) to volume=i,issue=j of the ACM SIGSOFT Software Engineering Notes. Most of those cases were initially discussed on-line; grep away if you want the original items.

Repeatedly detained (S 10 3, S 11 1), Terry Rogan wins rights violation

case (S 12 4); settles for \$55,000 (S 13 2)

Other cases of false arrest due to computer database use: C.R. Griffin

license not suspended; Sheila Jackson Stossier mistaken for Shirley

Jackson; two Shirley Jones, diff birthdays, 6", 70 lbs diff (S 10 3)

More computer-inspired false arrests, libel, etc. (S 12 3)

Michael W. Klein, mistaken identity due to outrageous mismatch (S 20 2:7)

Identical database record names cause nasty tax problem in Canada (S 12 4)

Two Belinda Lee Perrys share the same birthdate (S 21 4:13, [R 17 88](#))

Nonupdated stolen-car database; one owner shot, one roughed up (S 21 4:14)

Risks of naming files ``core" (S 21 2:18)

Risks of non-portable configuration files ([R 17 62](#))

Mistaken-identity nightmares: Foster, O'Connor, Taylor, Stapelton (S 13 2)

Richard Sklar falsely apprehended three times because of impostor (S 14 2)

Roberto Hernandez falsely jailed twice; won \$7000 first time! (S 14 5)

Joseph O. Robertson in for 17 months despite contrary evidence (S 14 5)

Martin Lee Dement 2 yrs LA County jail; fingerprint sys not used (S 14 6)

Another bogus identity: Teresa Stover alias' VA DMV license;

`perhaps thousands' of fraudulent licenses `bought'? (S 16 3)

Driver arrested in computer muddle: two cars with same plates (S 17 1)

Police raid wrong house (twice), due to uncorrected database

typo (S 17 1)

Two Russ Hamiltons with same birthdate; wrong one jailed (S 19 3:6)

Imposter usurps Clinton Rumrill's existence (S 19 3:7)

New license sent to imposter who plagued Charles Crompton (S 19 3:7)

Rented car falsely listed as stolen leads to false incarceration (S 16 4)

ATM photo of wrong person sent as rapist/robber; 'downloading error' (S 16 4)

Motorist gets citation based on photo, responds with photo of money (S 16 4)

Impersonator transfers numerous traffic citations to victim (S 17 2)

Two Steven Reids in Montreal sharing same birthday (S 18 1:22);
See also Don Norman, et al., on-line ([RISKS-14.12-17](#)) on Name Problems

Ignoring smart-card risks

David Randolph <daverand@nkn.net>

Mon, 17 Mar 1997 10:40:12 -0600

Recently, the Risks Forum listed an article describing successful attacks on smart cards. I reviewed the article and talked to a friend at a chip reliability lab. He believed that his lab could use those techniques to break the card security in a few days from a standing start. Once the system was up, they could do it in hours. Based on that, I believe that the challenges to smart cards are very real and that the cost of breaking a smart card is low enough to make it worth while for organized crime to use.

Card Technology magazine (intended for executives in the smart

card

arena) in the Jan/Feb 97 issue had an article titled ``Facing the Smart-Card Security Issue''. (Here are some selected quotes.)

"The industry needs to put the latest attacks and methodologies into

perspective by taking a good look at the security of their entire systems.

As we have heard before, any chain is only as strong as the weakest link.

This is definitely true for smart card systems. Most of the attacks of

recent days are classified as class 3 attacks, which means it would take

millions of dollars of equipment, and hundreds of years of computing power,

to actually break into a transaction. In most cases, there are many easier

ways for some of this information to be obtained. A thorough risk analysis

must be performed at every level of the system to determine what is being

protected, the value of that asset, and how much security is required to

protect that asset."

"The smart card is an intrinsically secure device."

"Are smart cards 100% secure? Claiming that any system and/or technology is

100% secure is irresponsible. Any system can be compromised given the

appropriate amount of resources. The main consideration for any system is

whether the level of security meets with the level of effort that an entity

would be willing to expend in order to compromise the security."

"Pay TV systems are probably the most publicized cases of security attacks

and compromises of smart cards. Once a pay TV system is compromised, new

cards are sent out to subscribers to update the system."

"A third paper was recently presented at the USENIX Electronic Commerce Workshop in Oakland, Calif. This paper "Tamper Resistance-A Cautionary Note" goes into more detail on how a smart card can be manipulated to produce a fault in a particular calculation. Its authors also have published a paper entitled "Improved Differential Fault Analysis" which reviews the work of both Bellcore and Shamir, putting it into a smart-card context."

The major risks are that people may believe that the smart card is still too expensive to break and thus not put in the checks to detect counterfeit cards. The risks are not in breaking one transaction, but in counterfeiting cards that the system can not detect are counterfeit. Whoever issued the original cards could wind up paying large sums to cover transactions from counterfeit cards. Visa recently ran a contest where the prize was a smart card containing \$2,500 value. That much benefit on one card makes the cost of counterfeiting look very attractive.

David Randolph Prairie Trail Software, Inc

[A smart card strategy may be to understand the risks of smart-card strategies. PGN]

Shockwave security hole exposes e-mail

Sidney Markowitz <sidney@research.apple.com>

Mon, 17 Mar 1997 10:41:05 -0800

Shockwave is a Web browser plug-in from Macromedia <http://www.macromedia.com> that plays animated multimedia content. A security hole that allows a Web server to read e-mail files on a client browser's machine is described by David de Vitry on <http://www.webcomics.com/shockwave/> with an example Web page that reads Netscape Navigator e-mail files on Windows 95 and NT, how Shockwave can be used to read any local file on the client machine and send data to the server, and Macromedia's response and plans for fixes. This site also gives yet another variation that allows the server access to any Website that the client has access to, even Websites on local networks and behind firewalls. See also <http://www.wired.com/news/technology/story/2548.html> . Another article at <http://www.macintouch.com> shows how the same technique can be used to read Eudora mail files on a Macintosh.

Relevant to the previous discussions on RISKS about Authenticode, de Vitry points out that users of Microsoft Internet Explorer who enter a page with a Shockwave movie on it are presented with an Authenticode digital certificate signed by Macromedia, not by the author of the possibly malicious movie.

-- sidney markowitz <sidney@research.apple.com>

[Sidney kept sending me later updates from Friday and Monday, which I have incorporated. The date/time stamp is from his latest message. PGN]

⚡ Risks of online commerce

"Paul O'Donnell" <pod@ms.com>
Mon, 17 Mar 1997 14:04:22 -0500 (EST)

A couple of weeks ago I tried to use www.movielink.com to purchase tickets for "The Empire Strikes Back" at a theatre in New York. I've used this service many times in the past (at other theatres). For those who haven't used it, it works over https - you select a movie showing, give it the number of tickets, credit card number and expiry date. It gives you a page saying "You must remain on this page", while it processes the transaction, and then gives a success or failure message. When you get to the theatre, you swipe your card in a card reader, and the tickets pop out.

For this movie, I got a failure message so I tried again. This too failed, so I gave up and bought the tickets the old fashioned way.

I just checked my credit-card bill, and I was billed (by the theatre, not some ticket agency) for both attempts. How many people keep an accurate track of the movies they saw a month ago?

[Especially risky if you see a lot of films. You may be suffering from Jedi Red-Eye, and spending too much time in E-Wok mode -- some sort of electronic Chinese-restaurant syndrome? PGN]

⚡ Experiences with a Year-2000 credit card

Robert Bowdidge <bowdidge@watson.ibm.com>

Sat, 15 Mar 1997 12:02:31 -0500

Well, I'm getting to experience the Year 2000 problem first-hand. My bank sent me a Visa debit card with an expiration date of January, 2000 last month.

I didn't notice the problem until I first tried to use the card. The local grocery store's card reader wouldn't handle it; when it phoned the bank, it came up with some error code the checker didn't know about, and wasn't about to try to figure out. At another store, the card reader also phoned the bank and came up with a strange error code. When the clerk phoned in the problem, he found the error message explicitly meant "your firmware is out of date, look in your manual for the process for upgrading the card reader's software."

I've also hit one store that has a combination cash register and card reader that appears to date from the early '80's. Their card reader caught the date problem before phoning in the card, and thus wouldn't allow the bank to be contacted. The clerk assumed the problem was a date problem and misread the "valid from" date as the expiration date in his quest for something that looked (to his eyes) as a valid date. The owner of the store didn't seem to understand my explanation for the problem, either.

In most of the cases where the card's been rejected, the clerk's been completely confused by the card reader's reaction and isn't sure what to do.

Luckily, by issuing error codes at the bank end on Y2K problems, the bank can probably figure out which card readers are running old software, then lean on the store managers to update the software. This minimizes some of the risks of untrained salespeople not understanding the problem enough to tell their manager to update the card reader.

I'm going to try very, very hard to have one card with a 1999 expiration date at all times for the next few months.

Debugging New York State one card reader at a time,

Robert

(Other RISKS articles about VISA's warnings to member banks:

[RISKS-18.62](#), "current score is Y2K 1, Visa 0",

[RISKS-18.74](#) "VISA fines banks with Y2K problems"

Other first-hand stories

[RISKS-18.65](#), "Year 2000 and expiration dates",

Salesmen canvassing for non-Y2K card readers

[RISKS-18.68](#), "Year 2000 Sharks")

[Another case forwarded to RISKS by tony.lima@toadhall.com (Tony Lima). PGN]

🔥 Re: Y2K: the revenge of originality (Vaneynde, [RISKS-18.90](#))

<amos@nsof.co.il-nospam>

Mon, 17 Mar 1997 14:58:37 GMT

> he told me of a colleague who used nonsense words as identifiers ...

Since COBOL has about 300 reserved words, a lot of programmers have taken to

using nonsense words for variable names, to avoid reuse of a reserved word.

This makes it much more probable that a date field would have a meaningless name, than in most other languages.

Amos Shapir nSOF Parallel Software, Ltd., Givat-Hashlosha
48800, Israel
amos@nsof.co.il +972 3 9388551

⚡ Risks of random-number servers (Re: Drake, [RISKS-18.90](#))

Eric Rescorla <ekr@terisa.com>

Mon, 17 Mar 1997 07:24:46 -0800

While I understand, quite easily, the feeling that one (or in this case one's friend) has tried to do a good deed and it hasn't gone unpunished, I nevertheless think Mr. Drake is missing the point -- which is that industrial-strength random numbers merit industrial-strength delivery.

The presumptive argument for this service is that the numbers provided by this system are better (more random) than the user could obtain on his own. While the source of these numbers may well be superior, the method of their delivery may well render them worse than the user could obtain on his own.

Mr. Drake says:

> The Risks question here is, just what level of paranoia is suitable here?

> If you're paranoid enough to think you need quantum-randomness as

> your random number source, you should definitely want extremely
> high security in how they are delivered.

Interestingly, this is the precise converse of the usual error:
getting your
crypto right and your randomness wrong. The risk, of course, is
the same:
lavishing care on one part of a security system while ignoring
the rest.

-Ekr [Eric Rescorla]

✶ Ariane 5 - a wry comment

"C. Shen Orr" <cshenorr@netvision.net>
Sat, 15 Mar 1997 09:44:55 +0200

The Ariane 5 failure surely is the winner of the ongoing contest
for "Most
Damage Done Per Line-Of-Code Changed" - \$1.8B / 0 [!].

I fully agree with Kevin Quinn's point ([RISKS-18.90](#)): no formal
methods
would have detected the problem - its roots lie within the realm
of human
communications and tying together seemingly-unrelated physical
information,
rather than programming.

[Coming through, awry? Comment by PGN]

✶ Re: Telephone Scam (Daniels, [RISKS-18.90](#))

Lou Fernandez <lff@sequent.com>
Mon, 17 Mar 1997 10:37:57 -0800

The house I live in (in Portland, Oregon, USA) was formerly owned by a family with many teenagers and a home-based business so they had at least 5 telephone lines. I have one phone line. However, I get a dial tone on 4 of the 5 lines coming into the house.

I believe this happens when the local telephone service provider does not physically disconnect the wiring when service is canceled. When they subsequently reassign a wire pair from the canceled service to a new customer, they make a new connection to the wire pair. Now the wire pair can be used by both the old and new customer and the new one gets the bill.

It's also possible the wires are accessible to people other than you and the phone company. If you live in an apartment building, the phone lines for all the residents probably are accessible from a single box in the basement. If that box is not sealed with a phone company seal, anyone with a telephone and access to the box could have made the calls.

Louis F. Fernandez Sequent Computer Systems Beaverton, OR 97006-6063
lfernandez@sequent.com

⚡ Re: Telephone Scam (Daniels, [RISKS-18.90](#))

<hicks@millcomm.com>

Fri, 14 Mar 1997 20:55:35 -0500

Many years ago, when I took up residence in New Jersey to work

for what was
then a major electronics company (and what is now a minor
subsidiary of GE),
I had some problems with the phone in my apartment. At first it
didn't work
at all, but the phone company was finally able to get it working
after about
ten days. It had bad crosstalk, but I took that to be a problem
with the
old lines in the area.

About a month later I got my first bill. There were toll
charges totalling
over a hundred dollars, even though I had only used the phone
for about ten
brief calls. I called the business office and got the usual
"the computer
doesn't lie" response. (Based on the numbers called, the
charges appeared
to be associated with a construction business, but the folks in
the business
office seemed unimpressed with the argument that I'd have no
reason to make
such calls).

Not knowing what else to do, I called the repair service and
complained that
the lines must be crossed somewhere . A few days later the
crosstalk
disappeared (and later bills revealed that the improper billings
ended on
the same date).

Unfortunately, the repair service didn't communicate any of this
to the
billing department, and I continued to be billed for the bogus
calls. Only
after I insisted that the folks in the billing department
inspect the
service records did they grudgingly agree to adjust my bill.

Risks: Obviously, the "the computer doesn't lie" syndrome.
Beyond that,

though, three more observations:

1) It is arguable that the repair personnel, when they corrected the apparent wiring error, should have recognized that it could have generated bogus billings and communicated this information to the billing department, especially since the service call was initiated with this suspicion.

2) Some consideration should be given in the design of equipment to the prevention of this sort of error. Close as I can tell, the problem was probably some sort of simple wiring error -- either a short between adjacent wires or a "split pair". That such a reasonably likely error could go undetected and, further, produce erroneous billings, indicates a lack of "robustness" in the design.

3) Consumers are increasingly at the mercy of various forms of automated, computerized billings, but increasingly there is no "hard copy" or independently verifiable record of the transactions. In a sense this is valid justification for an increasing level of technophobia.

Dan Hicks <http://www.millcomm.com/~danhicks>

✉ Re: Telephone Scam (Daniels, [RISKS-18.90](#))

Stuart Woodward <stuart@gol.com>
Mon, 17 Mar 1997 06:15:26 GMT

I don't think the following story will help solve the mystery of

the calls
to Guyana, but it demonstrates a risk with "intelligent" pieces
of telephone
equipment. I once found several calls on my International
telephone bill
that I was doubtful that I had made. Thankfully, they were all
very short.

The following month I called a friend in London, I was living in
Tokyo at
the time, but the call was answered by the operator who asked
which number I
was calling. Since I always used the single keypress quick dial
feature I
had difficulty in answering the question but looked in my
address book, told
the operator, and the call was put through. I asked my friend
why the calls
were being stopped and she said that they had been suffering
from calls
where no-one spoke.

Later, I noticed that there was an extra LED lit up on my answer
phone and I
looked in the (Japanese) manual to find out what it meant. It
meant that an
option designed to call a pager was enabled and that every time
someone left
a message on my telephone answering machine when I was out, the
telephone
was subsequently calling a pager number. I entered the sequence
to find out
what number it was calling and found that it was calling my
friends number
in London.

I then realized that a couple of months previously, when I had
first entered
her number as a single keypress number, it hadn't initially
worked and that
I had accidentally entered it as the pager call number. The key
sequences
do this were similar to the single keypress entry sequence.

Since I hadn't programmed a sequence to be sent to the pager, my telephone remained silent when it called my friends number. I didn't even know that the telephone had this feature as I only read the parts of the manual I was interested in.

The problem was hidden since it only occurred when I was not there to answer the call. Also the user interface of the telephone was very limited making it easy to make mistakes and hard to find them.

Had I been programming a single keypress dial number to a recorded service in London, I would possibly have run up an enormous bill.

⚡ Re: Telephone Scam (Daniels, [RISKS-18.90](#))

Pete Kaiser <kaiser@acm.org>
Mon, 17 Mar 97 14:31:26 +0100

This happened to me. A neighbor had made a physical tap into my phone line and used it to make many expensive long-distance calls. A switch cannot, of course, distinguish this from your own telephone, since it happens on the same wire. In my case it took several months, plus the threat of legal action, to persuade the telephone company to investigate the problem down to the level of the wires in my block of dwellings.

⚡ Re: Telephone Scam (Daniels, [RISKS-18.90](#))

"Jonathan I. Kamens" <jik@cam.ov.com>

Mon, 17 Mar 1997 14:01:06 -0500

If you are certain that the call was not made by someone in your house, then the two most likely explanations of their origin are:

1) You have a cordless phone, and someone with a similar model of phone made calls on your line from near your house (e.g., from a nearby house, or from a car parked nearby).

Some complicating factors:

Most cordless phones will not allow calls to be made when the handset is in the base. But you may have left the handset out of the base.

Before being able to do this, the thief would have had to figure out what model of cordless phone you had. But he could have seen you talking on your phone in your front yard, or he could live nearby and accidentally picked up a conversation on your phone, causing him to become aware of the fact that his handset is compatible with your phone.

Most cordless phones nowadays have some sort of security code exchanged by the handset and base before the base will allow a call to be made. But you may have a phone without such a system, or the attacker may have figured out (intentionally or accidentally as described above) the code used by your phone.

Of course, if you don't have a cordless phone, all of this is irrelevant :-).

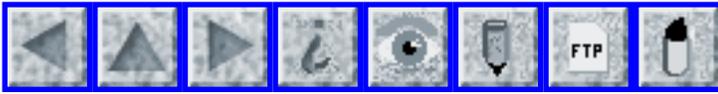
2) The thief tapped into your line outside the house to make the calls.

This isn't that hard to do. The telephone handsets used by repairmen are not that hard to come by, and all the thief would have to do is find the junction box for your telephone wires, open it, and clip a handset onto the line. Even if the junction box is inaccessible or locked, the thief could find the wires themselves, strip the insulation off of them, and clip directly to the wires.

If this is a possibility, then you should figure out where the wires for your phone line enter your house, and trace them back as far as you can (e.g., until they claim to the top of a telephone pole you don't want to (or aren't legally allowed to) climb). Make sure there's no place where the wires are stripped, and also make sure that any junction boxes and other wiring cabinets which provide access to the wires are locked.

If you find a junction box or wiring cabinet outside your house that isn't locked, you are almost certainly justified in calling CableTel and demanding that they (a) secure it and (b) don't charge you for the calls you did not make. However, they may have thought of this first, in which case they may have already sent out a repair crew to find your junction box and lock it.

Jonathan Kamens | OpenVision Technologies, Inc. | jik@cam.ov.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 18: Issue 92

Thursday 20 March 1997

Contents

- [Flaw in Cell-Phone Encryption Identified; Design Process Blamed](#)
[PGN](#)
- [The Illusion of Truth: Software Bugs as NewsBytes](#)
[Troy Heagy via Gary Grossoehme](#)
- [Bring me the head of InterNIC](#)
[Elizabeth Hanes Perry](#)
- [Bank cannot believe it made a mistake!](#)
[Glenn Story via PGN](#)
- [Accident at a nuclear waste processing plant: keeping log info handy](#)
[Chiaki Ishikawa](#)
- [Private information in Japanese Postal Service](#)
[Chiaki Ishikawa](#)
- [Taking cookies without asking permission](#)
[Shlomo-Zalman Jessel](#)
- [MS Internet Explorer for NT security hole](#)
[Mark Seecof](#)
- [Re: Y2K: the revenge of originality](#)
[Pete Kaiser](#)
- [Credit Cards and the year 2000](#)
[Lauren Weinstein](#)

- [Re: Telephone Scam](#)
[Bill Nugent](#)
[Jon S. Green](#)
 - [US FTC Workshop on Consumer Information Privacy](#)
[Denis McKeon](#)
 - [April 4 deadline of NSPW '97: Final Call for Papers](#)
[Yvo Desmedt](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ **Flaw in Cell-Phone Encryption Identified; Design Process Blamed**

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

Thu, 20 Mar 1997 12:35:16 PST

This is a press release <<http://www.counterpane.com/cmea.html>>
from

* Bruce Schneier, Counterpane Systems, 612 823-1098
schneier@counterpane.com

* David Wagner, University of California, Berkeley 510-643-9435
daw@cs.berkeley.edu

* Robert Sanders, University of California. Berkeley 510-643-6998
rls@pio.urel.berkeley.edu

* Lori Sinton, Jump Start Communications, 415-938-2234
lsinton@aol.com

Telecommunications Industry Association algorithm
for digital telephones fails under simple cryptanalysis

MINNEAPOLIS, MN. AND BERKELEY, CA., March 20, 1997 - Counterpane Systems and UC Berkeley jointly announced today that researchers have discovered a flaw in the privacy protection used in today's most advanced digital cellular phones. This discovery points to serious problems in the chosed-door process used to develop these privacy measures. This announcement is a

setback to the US cellular telephone industry, said Bruce Schneier of Counterpane Systems, a Minneapolis, MN consulting firm specializing in cryptography. The attack can be carried out in a few minutes on a conventional personal computer.

Schneier and John Kelsey of Counterpane Systems, along with graduate student David Wagner of the University of California at Berkeley, plan to publish their analysis in a paper entitled "Cryptanalysis of the Cellular Message Encryption Algorithm (CMEA)." Legislators are scheduled to hold hearings today on Rep. Goodlatte's "SAFE" (Security And Freedom Through Encryption) bill, HR695.

The problem affects numbers dialed on the key pad of a cellular handset, including any telephone, PIN, or credit cards numbers dialed. The system was supposed to protect the privacy of those dialed digits, but the encryption is weak enough that those digits are accessible to eavesdroppers with a digital scanner.

The cryptographers blame the closed-door design process and excessive pressure from U.S. military interests for problems with the privacy standard. The cellular industry attempted to balance national security with consumer privacy concerns. In an attempt to eliminate recurring security problems, the cellular standards arm of the Telecommunications Industry Association(TIA) privately designed this new framework for protecting

cellular phones. The system uses encryption to prevent fraud, scramble voice communications, and protect users' privacy. These new protections are being deployed in today's digital cell phones, including CDMA, NAMPS, and TDMA.

Not a new problem

As early as 1992, others - including noted security expert Whitfield Diffie - pointed out fatal flaws in the new standard's voice privacy feature. The two flaws provide a crucial lesson for policy makers and consumers, the researchers said. These weaknesses are symptomatic of broad underlying problems in the design process, according to Wagner.

Many have criticized the National Security Agency (the U.S. military intelligence agency in charge of electronically monitoring foreign powers) for insinuating itself into the design process, pressuring designers to cripple the security of the cellular encryption technique and hamstringing emerging cellular security technology. "The result is weaker protection for everybody," Kelsey said.

"This is another illustration of how U.S. government efforts to control cryptography threaten the security and privacy of Americans," said David Banisar, attorney for the Electronic Privacy Information Center in Washington, D.C.

This is not the first report of security flaws in cellular telephony. Today, most cellular phone calls can be intercepted by anyone in the area listening

to a scanner, as House Speaker Newt Gingrich learned this past January when someone with a scanner recorded one of his cellular calls. According to FCC estimates, the cellular telephony industry lost more than \$400 million to fraud and security problems last year.

CMEA Technology

CMEA is a symmetric cipher, like the Digital Encryption Standard (DES). It uses a 64-bit key, but weaknesses in the algorithm reduce the key to an effective length of 24 or 32 bits, significantly shorter than even the weak keys the U.S. government allows for export.

Greg Rose, program chair of the 1996 USENIX Security Symposium, put the results in context: This break does not weaken the digital cellular fraud protections. And it's still true that digital cellular systems are much harder to casually eavesdrop on than analog phones. But it's clear from this break that a determined criminal with technical resources can intercept these systems."

Counterpane Systems is a Minneapolis, MN-based consulting firm specializing in cryptography and computer security. Bruce Schneier is president of Counterpane and author of three books on cryptography and security. David Wagner is a founding member of the ISAAC computer security research group at UC Berkeley. In the Fall of 1995, the ISAAC group made headlines by revealing a major flaw in Netscape's web browser. The authors also hasten to thank Greg Rose for his advice.

[This was also noted by "Tom Zmudzinski" <zmudzint@ncr.disa.mil>.

Several others contributed John Markoff's article in *The New York

Times* today. As usual, my local source, *San Francisco Chronicle*,

ran the NYT item without indicating its author. PGN]

🔥 The Illusion of Truth: Software Bugs as NewsBytes

<GaryG4430@aol.com>

Thu, 20 Mar 1997 13:58:25 -0500 (EST)

This was posted on the rec.arts.sf.tv.babylon5.moderated group (Babylon 5 TV series) It is one of the most understandable passages on the problem I have seen. Actually several different problems. The Risk? The problem we are all vetting about may not be the underlying problem that will kill us.

Gary Grosseohme, Oregon Electronics, GaryG4430@aol.com

Date: 20 Mar 1997 00:08:06 -0500

>From: Troy_Heagy@ccmail.orl.lmco.com

Newsgroups: rec.arts.sf.tv.babylon5.moderated

Subject: "The Illusion of Truth" in action

Here is a good example of the press distorting the truth just as in the recent Babylon 5 episode, "The Illusion of Truth."

Hard Pressed

Tech journalists are more interested in crises like the Explorer bug than the fundamental problems behind them. Ever wonder how the news really works behind the scenes? I got a powerful firsthand lesson on 3 March,

when

Worcester Polytechnic student Paul Greene discovered that "serious flaw" in Microsoft's Internet Explorer. That's when I became the unwitting source of a sound bite that overshadowed the real news.

My first indication that something was up was an e-mail from Gene Spafford, who has been my co-author and editor on three computer-security books. Gene subscribes to bugtraq@netspace.org, a "full-disclosure" mailing list about hot computer security holes. The subject line was "FYI - browser bug." The message pointed to Greene's Cybersnot Web page.

As I read the message, my jaw dropped. "Cool," I thought. "I can run any program I want on anybody's computer who looks at my Web page with Internet Explorer." Sort of like ActiveX without the code-signing.

Five minutes later, my phone rang. It was Thomas Reardon, who works at Microsoft on IE. "I want you to know that this isn't an ActiveX problem," were the first words out of his mouth.

I told Reardon that I had read the Cybersnot message and didn't think that this IE problem was any more significant than the numerous security problems that have plagued Netscape's Java engine. After all, the Secure Internet Programming group at Princeton University had discovered a dozen or so ways of making Java Virtual Machines run arbitrary machine code. The only difference between their attacks and this one was that you needed to be fluent in Java bytecodes, x86 assembler language, and obscure type systems

in order to exploit the Princeton attacks. For the Greene bug, all you needed to know was HTML.

But Reardon was worried. He said that his co-workers at Microsoft were certain that the press was going to burn them alive. And the bug was so simple - just two flipped bits in IE's registry entries. Internet Explorer has a list indicating whether files are safe or dangerous to open, Reardon explained to me. URL files and LNK files had been listed as safe, meaning it's OK for IE to open them without first asking the user's permission. They should have been listed as dangerous.

Next, my pager went off. My friend Beth Weise, cyberspace correspondent for the Associated Press, wanted me to call another reporter and fill him in. I tried to stress to the reporter that the real problem wasn't Internet Explorer - it's the fact that people use the Windows operating system, which has no built-in security. "What we really need is secure operating systems, but corporate America doesn't buy them," I said. But that didn't make for a good story.

The AP story must have gone out over the wire about 10 minutes after I hung up the phone, because I had just sat down to dinner when my phone rang again. This time it was CBS Radio News. They wanted to do an interview-to-tape right then! So I told the guy from CBS the same thing I had told George from the AP. The impact of this bug, I said, was that it acted as if somebody were messing with your computer while you "went out to

lunch."

That "lunch" quote had wings of its own. Within the next 24 hours I was quoted on CNN, CNBC, National Public Radio, and in dozens of publications. The Seattle Times ran my quote. It was really weird, because the woman who wrote the story knows me, knows my home phone number, but she found it easier just to grab the quote from the AP than to call me up and get the story behind the sound bite.

This sort of quote reuse is actually typical for the nation's news services. I shouldn't be surprised. But I was upset that everybody focused on the immediate problem - a bug (oh no!) in Internet Explorer.

Nobody asked why today's computers are so brittle that a single bug could leave a Web surfer wide open to attack. Nobody made the connection between this bug in Internet Explorer and ActiveX. Microsoft goes to great pains to make sure that security-critical bugs like this don't slip into its applications, and yet this one did. What about signed ActiveX components? They're sure to have security-critical bugs as well - especially since many of them will be written in C++. This is a problem that Java applets simply don't have, because they run within the restricted sandbox environment.

Nobody seems to be looking to the future. We're building a wired world, but all those wires are crossed. We've had a lot of warnings. Pretty soon, we're going to start having disasters. It's time we started looking harder at the threats.

⚡ Bring me the head of InterNIC

<betsyp@vnet.net>

Thu, 20 Mar 1997 09:34:48 -0500 (EST)

Yesterday, InterNIC, having lost the receipts from my employer's domain registration, invalidated my employer's top-level domain. (Note that this mail is NOT sent from my employer's domain, but from my local ISP; I am not authorized to speak for my employer.)

Like many others in similar situations, our system administrator spent the entire day trying vainly to get in touch with a human being at InterNIC to correct the error. He was eventually successful, but only after 20 hours of "Internet death" during which all E-mail, FTP, and accesses to our Web page bounced.

Moral? A single point of failure is just as serious when the point of failure is an organization as when it is an hydraulic valve. Many companies now arrange for backup Internet access should their primary provider fail; as far as I know, there is no way to arrange for backup name service should InterNIC fail.

Elizabeth Hanes Perry

betsyp@vnet.net

✶ Bank cannot believe it made a mistake!

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

Thu, 20 Mar 97 9:53:28 PST

Mike and Shelly Steen of Santa Rosa CA made a deposit of \$3700 to their Bank of America account. The deposit was credited as \$37,000. When they repeatedly tried to convince BoA there had been an error, they were told that that it could not have been a mistake that size because it would have been caught by the bank's verification system. [Thanks to Glenn Story, who spotted this item in the Palo Alto Daily News, 19 Mar 1997, p.28.]

✶ Accident at a nuclear waste processing plant: keeping log info handy

Chiaki Ishikawa <Chiaki.Ishikawa@personal-media.co.jp>

Tue, 18 Mar 1997 12:32:20 +0900 (JST)

There was a small fire and subsequently a small explosion at a Japanese nuclear waste processing plant in Ibaraki prefecture, north east of Tokyo. You can probably read the latest info on <http://www.asahi.com> (a web site of Asahi Shimbun newspaper. I just checked this and information is available in English, too. It carried the ominous news that a very tiny amount of Cesium 137 was observed in a nearby observation facility. You may not want to keep a bookmark of a particular article you saw at Japanese newspaper sites, though. For reasons unknown to me, they tend to

recycle the same file name for different articles and throw away the old ones. So in a few days, the same URL often points to totally different news.)

Before getting to the core of the story, I have to explain something I learned from security management. I have been managing office internet firewall for sometime, and learned a great deal from the book, Internet Security and Firewall, by Bellovin and Cheswick. Some of the useful tips in the book was to log copious amount of info for analysis and to make sure that the log is available for later analysis after incidents. Technique for this includes recording in a safe machine within internal LAN, recording the log on a write once media, or even using a PC with a network card so that no one can "break" into the machine via network to tamper with the system log. These will make sure that log is tamper-proof and accessible after incidents occur.

Well, why am I saying this in relation to the accident at the processing plant? In the morning newspaper the day after the accident, I read that the plant managers could not figure out immediately if radio active material was released into the surrounding immediately. This is such an important thing and I was incredulous. Reading on, I found out this happened because of the following design and events:

- There are four radio activity sensors around the building to monitor the radio activity level in the surrounding to see if radio active material escapes the sealing of the building.

I think that it is a good thing they have four such meters.

- But, these monitoring data are gathered and displayed in the monitoring room of the processing plant building, but *only* there.

- Because of the small fire and the smoke that erupted, the operators

had to be evacuated, and after the small explosion (most likely an

incident where the high-pressure within the sealed confinement of

the building punched holes via weak windows, doors and such) that

took place hours after the initial fire,

nobody could return to the control room to check out the meters.

So the four meters were running to check the radio activity levels and sent

data to the control room, but nobody could read it. I think extra sensor

devices were brought in when the deficiency was realized by the top brass at the plant.

I believe the designers of the processing plants took note and plan a revision of their monitoring systems very soon now.

After writing all this, I am planning to do some sort of dry run to see if

my firewall system can be restored in a quick manner if a disk drive is

disconnected and such. There is a Japanese saying that goes something like,

"Correct yourself by looking the behavior of others". I took due note of it.

(As far as the incident goes, it is rumored to be level 3 in the nuclear

incident scale in which 1 is the lightest and the worst is level 8. Chernobyl was level 8 and Three Mile Islands was level 5.

Because of the expanding warm gas of the fire and smoke and such, the air conditioners to keep the internal pressure lower than external (to prevent leakage) could not keep running and when they failed, adjacent rooms got contaminated one by one. One incredibly stupid thing that happened was that apparently the initial small fire probably caused by the high-temperature asphalt was not put out completely and led to the small "explosion" that tore holes in the supposedly sealed walls. Coupled with the deliberate lies that were aired to the public when a nuclear breeder reactor Monju had a major accident of releasing hot melting Sodium outside its secondary cooling system, the half public/half private corporation which controls the nuclear power reactors research and waste disposal is under heavy media criticism in Japan right now. Their inept handling of PR this time around by inexperienced engineer turned PR people added fuel to the criticism. I think we can learn a lot from efficient American PR people here: I am saying this with a tongue in cheek.)

✂ Private information in Japanese Postal Service

Chiaki Ishikawa <Chiaki.Ishikawa@personal-media.co.jp>

Tue, 18 Mar 1997 12:32:20 +0900 (JST)

Regarding the slippery handling of private information such as one's signature information by US Postal Service (or was it Post Office), I often

ask myself whether it can happen to us in Japan whenever I read such articles in RISKS.

Well, just this morning Mar 18, I read in Asahi Shimbun newspaper (Yokohama edition) that Japanese Postal Service will offer tracking services for some special services such as registered mails and such starting June 1st via network. That is a good news. I think they are motivated by the success of FedEx and other private courier services.

But I was thrilled after reading some details. According to the article, customers can type in the number assigned to the package to find out where it is going and other pertinent information: I mean if I read the article correctly, it seems that the system gives out the information of the addressee(!) WITHOUT any authentication whatsoever! I wish I am mistaken here. Maybe the number itself has some extra field that authenticate the validity of the number as known only to the holder of the assigned number?

In any case, I can't wait to mistype a digit/letter of an assigned number to MY package to see if it will print out someone's supposedly private info.

(I checked the Ministry of Post and Telecommunication's web page for more info:

<http://www.postal.mpt.go.jp/>

Unfortunately, I could not find the details about the tracking service although the page has the mailto: to solicit a catchy name for this new

tracking service from the public.)

Chiaki Ishikawa, Personal Media Corp., Shinagawa, Tokyo, Japan
142
ishikawa@personal-media.co.jp or Chiaki.Ishikawa@personal-media.
co.jp

✦ Taking cookies without asking permission

Shlomo-Zalman Jessel <mss@pluto.mscc.huji.ac.il>
Tue, 18 Mar 1997 16:58:04 +0200 (WET)

I recently received this notice from a friend:

I just downloaded Netscape Navigator 4.0 preview release 2. At long last, Navigator has an option that will block all cookies without popping up a warning for each one. It is in Edit->Preferences->Advanced. It seems to work properly, too!

Curiously, when I installed it it ignored my current setting (Always warn before accepting a cookie) and set me up with "Always accept cookies."
Users upgrading should be aware of this.

Faculty of Medicine, School of Occupational Therapy, Hebrew University /
Hadassah Hospital P.O. Box 24026, Mount Scopus Jerusalem 91240
Israel

✦ MS Internet Explorer for NT security hole

Mark Seecof <Mark.Seecof@latimes.com>

Mon, 17 Mar 1997 15:00:29 -0800

At <<http://www.efsl.com/security/ntie>> a description may be had of YASH in MS-IE, this time involving the silent disclosure of user/"domain"/machine identity info and a transform of the user's "domain" password which could be used for false-presence attacks or offline cracking.

Mark S. (Disclaimer removed)

✶ Re: Y2K: the revenge of originality

<Kaiser@acm.org>

Tue, 18 Mar 97 09:36:45 +0100

Amos Shapir notes that many COBOL programmers use "nonsense words for variable names, to avoid reuse of a reserved word."

It seems to me this is a problem principally for badly documented programs -- in my experience, the majority. It's hardly limited to Y2K problems.

Yesterday I talked with someone who told me about a crucially important program his company uses: it's years old, is utterly undocumented, and was created by a brilliant programmer who was with the company for many years until recently he committed suicide. Now, and only now, they're trying to figure out what to do about the program. Oh, yes: undocumented and written in assembler code. I wish them well.

Pete kaiser@acm.org

✶ Credit Cards and the year 2000 (Re: Bowdidge, [RISKS-18.91](#))

Lauren Weinstein <lauren@vortex.com>

Tue, 18 Mar 97 00:14 PST

It's worth noting that at least some banks are attempting to get a handle on this problem, now that cards expiring in 2000 and beyond are actually appearing... Wells Fargo, for example, sent a letter to merchants requesting that they attempt a particular "fictitious" transaction, and noted what the various return codes would indicate. In case of a year 2000 problem, the merchant is supposed to contact the bank and eventually receive (for a fee, of course, in most cases) firmware/software upgrades. Naturally, this doesn't do anything right away for the folks who already have the dreaded "00" expiration cards during this early phase of the transition period.

--Lauren-- Moderator, PRIVACY Forum www.vortex.com

✶ Re: Telephone Scam (Fernandez, [RISKS-18.91](#))

Bill Nugent <whn@topelo.lopi.com>

Wed, 19 Mar 1997 20:24:05 -0500

Phone companies are pretty good about catching lines that are disconnected.

More likely this is a life-safety regulation. In Massachusetts the

telephone company can not turn off dial tone on disconnected service because of the risk to life safety. These 'disconnected' phone numbers can only call 911, the operator, and the NYNEX business office (for new service).

Bill

✉ Re: Telephone Scam (Daniels, [RISKS-18.90](#))

Jon S Green <jonsg@harlequin.co.uk.NO.SPAM>

Tue, 18 Mar 1997 09:57:49 GMT

In [RISKS-18.90](#) Dewi Daniels describes a problem where calls to Guyana were billed to his telephone account, apparently in error. This neatly dovetails with a report on the BBC TV programme "Watchdog" which showed that a number of British Telecom customers had suffered similar problems. Although the reason was never fully established, one conjecture was that BT employees with access to calling card details had used them illegally to call overseas premium-rate phone-sex lines.

Jon jonsg@harlequin_co_uk See <http://pobox.com/~jonsg/junkmail.html>

✉ US FTC Workshop on Consumer Information Privacy

Denis McKeon <Dmckeon@swcp.com>

Wed, 19 Mar 1997 10:46:46 -0700

The following is condensed from:

<a href="<http://www.ftc.gov/os/9703/privacy.htm>">

FTC: Public Workshop on Consumer Information Privacy

thanks to a pointer in news.admin.announce

by "russ-smith" of <http://www.consumer-info.org/>

Written comments (paper/disk) are due by April 15
for the June 10-13 workshops in Washington, DC.

=====

SUMMARY: The Federal Trade Commission has determined to hold a public workshop devoted to consumer information privacy. The workshop will be divided into three sessions.

Session One is intended to gather information as part of a Commission study of the collection, compilation, sale, and use of computerized data bases that contain what consumers may perceive to be sensitive identifying information, often referred to as "look-up services." These data bases typically are used to locate individuals or develop individual background information.

...

Session Two will address recent developments in the collection, compilation, sale, and use of personal information online generally, including self-regulatory efforts, technological innovations, and unsolicited commercial e-mail. Session Three will address the same developments as they pertain to children's personal information.

⚡ April 4 deadline of NSPW '97: Final Call for Papers

"Dr. Yvo Desmedt" <desmedt@blatz.cs.uwm.edu>

Wed, 19 Mar 1997 18:36:40 -0600

[See [RISKS-18.69](#) for earlier message. PGN]

FINAL CALL FOR PAPERS, NEW SECURITY PARADIGMS '97

A workshop sponsored by ACM and the University of Newcastle upon Tyne.

Langdale Hotel, Great Langdale, Cumbria, UK
23 - 26 September 1997

More information will be provided on-line as it becomes available.

E-mail to:	newparadigms97@opengroup.org
use anonymous FTP from:	ftp.cs.uwm.edu
in directory:	/pub/new-paradigms
Use World Wide Web from:	http://www.cs.uwm.edu/~new-
paradigms	



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 18: Issue 93

Monday 24 March 1997

Contents

- [Splendour of the Seas not so Splendid](#)
[Mich Kabay](#)
- [County Data Trouble](#)
[Dave Rand](#)
- [Bill Would Outlaw Online Gambling](#)
[Edupage](#)
- [Legal action against Internet provider affects customers](#)
[Klaus Johannes Rusch](#)
- [Austria to disconnect from Internet on March 25](#)
[Gary Beckmann](#)
- [On looking before you leap?](#)
[Dick Mills](#)
- [The Year 2000 Problem -- a new principle for Y2K tools](#)
[Thomas Reps](#)
- [Retiring hardware after Y2K](#)
[Matt Welsh](#)
- [Virtual Real-Estate](#)
[Tony Lima](#)
- ["The Illusion of Truth" in action: apology to Simson Garfinkel](#)
[Troy Heagy](#)

- [Net random-number server](#)
[Stefek Zaba](#)
 - ["Emergency" Web Access!](#)
[Robert J. Woodhead](#)
 - [Re: Telephone Scam](#)
[James Byers](#)
 - [Area code split and verification](#)
[Alan K. Jackson](#)
 - [Re: Risks of online commerce](#)
[Bob Frankston](#)
 - [1997 IEEE Symposium on Security and Privacy program](#)
[Mike Reiter](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ **Splendour of the Seas not so Splendid**

"Mich Kabay [NCSA]" <Mich_Kabay@compuserve.com>

Mon, 24 Mar 1997 05:19:27 -0500

The Canadian `_Globe and Mail_` newspaper (97.03.22, p. A17) reports that computerization hit choppy waters on a recent cruise:

Splendour on the seas:

As we learned one evening, computer problems aren't the sole domain of land lubbers. Nowadays, everything is run by the darned things -- even cruise ships.

By Helga Loverseed

An after-dinner power failure was probably not what the captain had in mind as part of our evening's entertainment, but just as we were downing our dessert, there was an ominous thump and we were plunged into darkness.

The author makes the following key points:

- * Splendour of the Seas is a fully computer-dependent cruise ship.
- * After 8 months trouble-free, the ship developed "computer problems" when it sailed through the Caribbean.
- * The author writes that "the computers evidently didn't like the hot, humid climate."
- * The computer failure lasted 2 hours; during that time, the ship was dead in the water.
- * In addition, lights were dim, air-conditioning was off, and toilets wouldn't flush.

This behemoth is 11 stories tall, 112 metres long, and 35 metres wide. It houses 2,077 passengers and 723 crew and includes amenities such as a jogging track, shopping, movies, bars, and even an 18-hole miniature golf course. The ship depends on computer-driven stabilizers to control roll in rough seas.

[Comments by MK:

If the main screws and the ship's toilets don't work without computer control, what else is computer controlled? Navigation? Communication?

Why was the time to repair two hours? Are there no backup systems or were the backup systems also down?

If anyone has more information about this incident, please contribute to this thread.

As for me, I hope the ship's officers test its computers to see if they are Year-2000 compliant ...

Mich

M. E. Kabay, PhD, CISSP (Kirkland, QC), Director of Education National Computer Security Association (Carlisle, PA) <http://www.ncsa.com>

[I suppose it might add to the hypothetical risks if the ship were to cross the equator for the first time precisely at the Y2K midnight! PGN]

County Data Trouble

Dave R <daverand@nkn.net>

Mon, 24 Mar 1997 08:37:58 -0600

>From *The Dallas Morning News*, 24 Mar 1997, datelined Lubbock, TX:

A cranky county computer has resulted in some minor traffic scofflaws being listed in official records as drug offenders, child molesters, or burglars, according to the *Lubbock Avalanche-Journal* (23 Mar 1997). Apparently, the computer has been mismatching the names and charges of some defendants, including one man who was cited for not wearing a seat belt but listed in the county computer as an accused child molester. Officials at Ki Corp., which developed the software, insist that the computerized criminal record has complete data integrity.

[whatever that means! PGN]

✦ **Bill Would Outlaw Online Gambling (Edupage, 23 March 1997)**

Edupage Editors <educom@elanor.oit.unc.edu>

Sun, 23 Mar 1997 15:35:44 -0500

Sen. Jon Kyl (R-Ariz.) has introduced the Internet Gambling Prohibition Act of 1997, which would make illegal the transmission of any information related to gambling, including bets, wagers or the chance to win a prize or lottery. "We don't ask ISPs (Internet service providers) to be law enforcers, constantly checking sites," says Kyl. Rather, ISPs would be asked to cut off Internet access only following a written notice from a law enforcement agency. The ISP would not be liable for any damages, penalties or forfeiture resulting from the perpetrator's gambling operation. (BNA Daily Report for Executives 20 Mar 1997; Edupage, 23 March 1997)

[Don't bet on it. PGN]

✦ **Legal action against Internet provider affects customers**

Klaus Johannes Rusch <e8726057@student.tuwien.ac.at>

Sat, 22 Mar 1997 18:02:38 CET

On 20 Mar 1997, all computer equipment at an Internet provider's office, VIP, was confiscated by the police following an order by judge Helene

Partik-Pable, who has been investigating a charge against persons unknown regarding the distribution of material containing child pornography more than a year ago. It should be stressed that the provider, VIP, is not subject to any legal action, the confiscation is for evidence only.

Both the office rooms and the private homes of the owners were searched, and all equipment, including private computers, office equipment which was not even connected to Internet and computers which customers had placed at the ISP's location and backup tapes, were unplugged (rather than properly shut down) and taken away.

Consequently, about 2500 customers have no connection to Internet any more, nor access to their business data and private e-mail.

References (in German):

[1] Martin J. Laubach <mjl@tick.cslab.tuwien.ac.at> on <news:at.general>

[2] DER STANDARD, March 22, 1997, <<http://www.derstandard.at/>>

Klaus Johannes Rusch e8726057@student.tuwien.ac.at,
KlausRusch@atmedia.net
<http://www.atmedia.net/KlausRusch/>

[Check out the full press release [1] which was also sent to RISKS
by Martin Laubach. PGN]

✶ Austria to disconnect from Internet on March 25

Gary Beckmann <gary@radionics.com>

Mon, 24 Mar 1997 17:18:36 -0500

[I'm summarizing several reports I read in German.]

All the ISPs in Austria are going to pull the plug on the Internet on Tuesday, 25 Mar 1997 from 16:00 to 18:00 MET. This action is being taken to protest the seizure of all the computer equipment of an ISP named ViP last Thursday. [...text duplicating previous message omitted...] The ISP cannot even begin to calculate the financial losses they will post due to this action.

There is some disagreement among the Austrian ISPs as to the results of the planned Internet disconnection (A Land Goes Offline), ranging from those that worry about their contracts guaranteeing net access to those who feel that two hours is nothing -- even one day would be barely enough to express their outrage. But all the ISPs have apparently agreed to the two-hour protest shutdown.

[The risks of having agencies that don't understand the technology trying to control it have been gone over again and again. This is the first time, though, that I've heard it going to this extreme. It will be interesting to see what the results of the protest are. --gb]

⚡ On looking before you leap?

Dick Mills <dj.mills@pti-us.com>

Fri, 21 Mar 1997 15:26:08 -0500 (EST)

I attended a firefighter's training drill this week. We heard from a gas/electric company representative. He related the following anecdote.

The gas company was called to a house in Albany, NY to respond to a complaint about a carbon-monoxide alarm activating. When the serviceman questioned the woman of the house about the circumstances, she said that the alarm had been sounding since the night before. Astounded, he asked why she hadn't called immediately. She replied, "My husband charged upstairs to surf the internet for information about what to do about carbon monoxide in the house. I'm still waiting for an answer."

The Risk? Letting one's mind roam cyberspace while forgetting that our bodies remain in corporeal space. Personally, I vow to never send the message, "FIRE! FIRE!" via e-mail.

Dick Mills +1(518)395-5154 <http://www.pti-us.com> aka dmills@albany.net

⚡ The Year 2000 Problem -- a new principle for Y2K tools ([RISKS-18.53](#))

Thomas Reps <reps@cs.wisc.edu>
Fri, 21 Mar 1997 20:09:19 -0600 (CST)

Back in October, PGN posted the following note to the RISKS newsgroup.

>> I ran into Tom Reps this morning in San Francisco ... Tom

has been

>> chartered by DARPA to make serious recommendations on the Year-2000 problem.

I would like to bring one of the results that came out of this to the attention of RISKS readers.

As PGN indicated, the Defense Advanced Research Projects Agency (DARPA)

asked me last summer to help them plan a project aimed at reducing the

impact of the Year 2000 (Y2K) problem on the Department of Defense. DARPA

was particularly interested in whether there were "any techniques in the

research community that could be applied to the Y2K problem and have impact

beyond present commercial Y2K products and services". The most exciting of

the ideas that turned up concerns a method for using path profiling as a

heuristic to locate some of the sites in a program where there are

problematic date manipulations. It works as follows:

In path profiling, a program is instrumented so that the number of

times each different loop-free path executes is accumulated during an

execution run. With such an instrumented program, each run (or set of

runs) of the program generates a path spectrum for the execution --- a

distribution of the paths that were executed. Path spectra can be

used to identify paths in a program that are good candidates for being

date-dependent computations by finding differences between path spectra from execution runs on pre-year-2000 data and post-year-2000

data. By choosing input datasets to hold all factors constant except

the way dates are used in the program, any differences in the spectra obtained from different execution runs can be attributed to date-dependent computations in the program. Differences in the spectra reveal paths along which the program performed a new sort of computation during the post-year-2000 run, as well as paths --- and hence computations --- that were no longer executed during the post-year-2000 run.

With some further analysis of the spectra, for each such path that shows up in the spectral difference, it is possible to identify the shortest prefix that distinguishes it from all of the paths in the other path set.

For the Y2K problem, the path-spectrum comparison technique may provide help with two aspect of the problem:

- (i) determining the sites at which date-manipulation code occurs, and
- (ii) post-renovation testing.

Of course, the path-spectrum comparison technique is not guaranteed to uncover all sites of date manipulations. No technique can do this; all one can hope for are good heuristics. However, because path-spectrum comparison involves a different principle from the principles that lie behind the heuristics used in commercial Y2K tools, it should be a good complement to current techniques.

Furthermore, the path-spectrum comparison technique is actually applicable to a much wider range of software-maintenance problems than just the Y2K problem; it offers new perspectives on program testing, on the task of

creating test data, and on what tools can be created to support program testing.

This work is described in the following paper:

Reps, T., Ball, T., Das, M., and Larus, J., "The use of program profiling for software maintenance with applications to the Year 2000 Problem". Technical Report TR-1335, Computer Sciences Department, University of Wisconsin, Madison, WI, January 1997.

The paper is available over the WWW at URL <http://www.cs.wisc.edu/wpis/papers/tr1335.ps>.

A prototype tool for gathering and comparing path spectra (for programs that run under Solaris on Sun SPARCstations) has been built at the University of Wisconsin.

(The Wisconsin Alumni Research Foundation is in the process of seeking patent protection for these techniques.)

Tom

⚡ Retiring hardware after Y2K

Matt Welsh <mdw24@cl.cam.ac.uk>
23 Mar 1997 12:43:52 GMT

In 18.90, Geoffrey Cooper writes:

>We decided to retire the product in (or at least upgrade the flash ROM >by) the year 2037.

I hate to point this out, but this is exactly the mentality that caused the Y2K problem in the first place. How do you know that all of these devices will be out of use by 2037?

It seems that people can either fix the problem, or ignore it, or pretend to fix it and give themselves a good pat on the back for doing so.

M. Welsh, Cambridge Computer Laboratory

✶ Virtual Real-Estate

Tony Lima <tony.lima@toadhall.com>
Sun, 23 Mar 1997 20:34:00 -0700

In the San Francisco area, Coldwell-Banker is running an ad for their real-estate services. This ad shows a woman worrying about how she will be able to keep the house clean while it is for sale, what with their three kids, two dogs, and so on. Her solution? Coldwell-Banker puts their house on the Web, keeping it (virtually) spotless. The risks are obvious. Next step: virtual patching of that cracked foundation...

tony.lima@toadhall.com (Tony Lima)

[I'd be just as suspicious of Real Virtual-Estate. PGN]

✶ "The Illusion of Truth" in action: apology to Simson Garfinkel

<Troy_Heagy@ccmail.orl.lmco.com>

Mon, 24 Mar 1997 12:14 -0500 (EST)

Last week I posted a message in the Usenet newsgroup rec.arts.sf.tv.babylon5.moderated. The message was then forwarded to the RISKS digest by someone else who was browsing through the newsgroups.

It looked as if I had written the article, but I did NOT. The author of that column, "Hard Pressed," was Simson Garfinkel. His Webpage address is <http://www.packet.com/garfinkel> .

"Hard Pressed" reminded me of the recent episode "Illusion of Truth"...how the press reports what it wishes rather than what you actually say...and I wanted to pass it on to Babylon 5 fans. Rather than quote the entire article I should have listed Simson's web page address. OR asked his permission to quote. I did neither.

I apologize to Simson Garfinkel and the readers of the Risks Digest for infringing on his copyright and for the misunderstanding this caused.

Troy_Heagy@ccmail.orl.mmc.com

[Your moderator is astounded, mortified, and apologetic that the obvious self-references pointing to Simson as the creator of that piece (coauthor of books with Spaf, friend of Beth Weise, etc. -- I had seen Simson and Beth at CFP just the week before) did not set off alarm bells and cause me to reject the message as a clear copyright violation. However, I somehow missed them when selecting that item. The volume of RISKS e-mail is

enormous, RISKS is a pro bono effort, and this piece was really good based

on a fast review for content that incredibly did not pick up on the

omitted true identity of the author! Besides, Simson has been occasionally sending me heads-up notices on his particularly-relevant

Wednesday packet columns at <http://www.packet.com/garfinkel>, for possible

mention in RISKS, but he did not so so on this seemingly relevant column.

So, my apologies as well as Troy's. We also received some groveling

from Gary Grossoehme, who, unknowing, submitted the item to RISKS.

In any event, this does remind us once again of the risks of enforcing

copyrights and the importance of netiquette in attributions. That even

gives me a chance to remind you to check the RISKS reuse policy in

<http://www.csl.sri.com/risksinfo.html> if you rebroadcast RISKS items! PGN]

⚡ Net random-number server

Stefek Zaba <sjmz@hplb.hpl.hp.com>

Mon, 24 Mar 1997 22:13:08 +0000

Among the risks not yet mentioned is the one of using an observable quantity

directly as (for example) keying material. Since the link to the hotbits

site is not encrypted, anyone with a machine sharing the transmission medium

can see what the random bits are. The cautious crypto-oriented user of this

service will mix the bits from the net.randomness server with

some locally-generated non-predictable bits; however, the incautious might not, and in any case if a local source of non-predictable (and non-observable) bits is available, using an external non-predictable but observable source adds only the illusion of security. (There are unusual applications where non-predictability is all that's needed, and observability is irrelevant; but it's not the common case.)

If this service were to be used for crypto applications, the bits would need to be not just PGP-signed, as Dan Drake suggested, but encrypted. PGP use would require the requester to send a public key with the request; SSL would allow the secure channel to be set up with less manual intervention.

Stefek stefek_zaba@hplb.hpl.hp.com

⚡ "Emergency" Web Access!

"Robert J. Woodhead (AnimEigo)" <trebor@animeigo.com>

Fri, 21 Mar 1997 16:40:03 -0500

Like many people, I use a PPP modem-dialup to an ISP to access the net from my portable computer. Usually this is a local call, but occasionally when travelling I have to make a quick long-distance call to get my email.

Recently I was at the video studio subtitling samurai films when the urge to check email became too much. The studio had a new phone system, so I found

out what the outside line prefix was, adjusted my PPP settings,
and happily
TCP/IP'd.

The next day, back home, I plugged in my Mac and dialed up - but
forgot to
revert my settings. I dialed, immediately noticed the problem,
and aborted
the attempt.

30 seconds later, the phone rang - it was 911 asking why I'd
called!

My video studio had chosen "91" as their outside dialing
prefix. And, of
course, I then needed to have my modem dial 1 for long distance
access, thus
putting in place a little time bomb for when I returned home!

Whoever came up with the idea of 91 as a dialing prefix ought to
be stuffed
and mounted!

Robert J. Woodhead ** trebor@animeigo.com ** "Anime Your Way!" tm
WWW.ANIMEIGO.COM - "REGULAR" and "LITE" flavors - CHAT room too!

[Another variant on an old RISKS theme. PGN]

⚡ Re: Telephone Scam (Nugent [RISKS-18.92](#); Fernandez, [RISKS-18.91](#))

James Byers <jwb19@cornell.edu>
Mon, 24 Mar 1997 15:00:36 -0500

Bill Nugent correctly points out that many telcos leave
dialtones on
disconnected lines for safety reasons. However, our local phone
company was
prone to crossing their lines in their jumble of antique phone

equipment.

Several years ago, I mistakenly attached a phone to a disconnected line. As realized my mistake later that day, the phone rang! I did not pick the phone up, thinking that the call belonged to someone else. It rang about four times and then stopped. Curiosity got the better of me and I dialed the operator from the phone a few minutes later. I told the operator that I was at a pay phone that was not labeled and I wanted to know the number.

"You're at a coinbox?" she replied incredulously. With my affirmative reply, she gave me the number.

I dialed the phone from another line and, sure enough, my phone rang four times and an answering machine picked up. Apparently, our disconnected phone was crossed with a local construction company! The phone company representative who got to hear this story tried to convince me that that I was imagining things. The representative also refused to believe that an operator would give me the number of a domestic phone. Not surprisingly, there was a repair truck out on the street the next morning. Funny coincidence, the line got disconnected at about the same time.

The risks? Certainly there are billing issues here that could cause someone quite a headache. Had I been a more malicious individual, I could have lost the construction company a fair bit of business. The operator also disregarded whatever indications she had that I was not on a pay phone. What would she have done if I had convincingly argued that I was

a repairman
and needed some sort of special phone access? Another case of a
human
operator disregarding both training and diagnostic indicators.

James Byers byers@cornell.edu [http://www.people.cornell.edu/
pages/jwb19](http://www.people.cornell.edu/pages/jwb19)

⚡ Area code split and verification

"Alan K. Jackson 245-7355" <ajackson@shellus.com>
Mon, 24 Mar 1997 07:40:59 -0600

Houston split its area code a few months ago, and we are
beginning to
experience many problems. The latest - my wife received a new
credit
card. She called the number to enable the card, and it failed
because the
number in their database didn't match the number she called from
- wrong
area code!

The risk - the credit card issuer will certainly lose some
business, anyone
not willing to spend the time to get a human to enable the card.

In general, this is a problem with the burgeoning systems that
take
advantage of the ease with which one can now trap the number of
an incoming
call. One's database of numbers can very quickly become badly
out of date.

⚡ Re: Risks of online commerce

<Bob_Frankston@frankston.com>

Mon, 24 Mar 1997 18:40 -0500

The problem of remembering purchases you made a month ago is one I specifically dealt with in my Masters Thesis (URL on request -- I'm on a plane so can't check it) in 1974. The basic approach is to keep a personal log of all transactions and automatically check the bill against these to note exceptions. The assumption is that there would be too many microtransactions to be able to check them all, especially when there is a delay.

Implementing this would require a payment system with a standard client-side component. Something that is difficult in today's decentralized marketplace.

🚀 1997 IEEE Symposium on Security and Privacy program

Mike Reiter <reiter@research.att.com>

Mon, 24 Mar 1997 14:34:44 GMT

1997 IEEE SYMPOSIUM ON SECURITY AND PRIVACY

May 5-7, 1997

The Claremont Resort, Oakland, California

Sponsored by the IEEE Technical Committee on Security and Privacy
In cooperation with the International Association of Cryptologic
Research

Symposium Committee:

Stephen Kent, General Chair

Michael Reiter, Vice Chair

George Dinolt, Program Co-Chair

Paul Karger, Program Co-Chair

PRELIMINARY PROGRAM
Subject to Change

Sunday May 4, 1997 4:00-7:00 Registration and Reception

Monday May 5, 1997

8:30 Introductory Remarks

9:00-10:30 Panel/Debate

Resolved: The concept of Trusted Computing Base as a basis for constructing systems to meet security requirements is fundamentally flawed and should no longer be used to justify system security architectures.

Arguing in favor: Lead: Bob Blakley (IBM)
Second: Darrell Kienzle (U. of

Virginia)

Opposed: Lead: William R. Shockley
Second: LT (USN) James P. Downey
(Naval Postgraduate School)

Moderator: John D. McLean (Naval Research Laboratory)

11:00-12:00 Authorization and Authentication

Toward Acceptable Metrics of Authentication

Michael K. Reiter and Stuart G. Stubblebine (AT&T Labs--Research)

An Authorization Scheme for Distributed Object Systems

V. Nicomette and Y. Deswarte (LAAS-CNRS & INRIA, France)

A Logical Language for Expressing Authorizations

Sushil Jajodia (George Mason University), Pierangela Samarati

(Universita' di Milano) and V. S. Subrahmanian (University of Maryland)

1:30-3:00 Applications

Anonymous Connections and Onion Routing

Paul F. Syverson, David M. Goldschlag and Michael G. Reed (Naval Research Laboratory)

The Design and Implementation of a Multilevel Secure Log

Manager

Vikram R. Pesati, Thomas F. Keefe and Shankar Pal (Penn State University)

A Secure and Reliable Bootstrap Architecture

A. Arbaugh, David J. Farber and Jonathan M. Smith
(University of Pennsylvania)

An MBone Proxy for an Application Gateway Firewall

Kelly Djahandari and Dan Sterne (Trusted Information Systems)

3:30-5:00 Security Theory

Secure Software Architectures

Mark Moriconi, Xiaolei Qian, R. A. Riemenschneider (SRI) and

Li Gong (JavaSoft)

A General Theory of Security Properties and Secure Composition

A. Zakinthinos and E.S. Lee (Cambridge University, U.K.)
Analyzing Consistency of Security Policies

Laurence Cholvy and Frederic Cuppens (ONERA CERT, France)

6:00-7:30 Reception

Tuesday May 6, 1997

9:00-10:30

Panel: Ensuring Assurance in Mobile Computing

Moderator: Marv Schaefer (Arca)

Panel Members: Sylvan Pinsky (NSA)

Drew Dean (Princeton University)

Jim Roskind (Netscape)

Li Gong (JavaSoft)

TBD (Microsoft)

11:00-12:00 Architectures

Packet Filtering: Local Enforcement for Global Policies

Joshua D. Guttman (MITRE)

Providing Flexibility in Information Flow Control for Object-Oriented Systems

Elena Ferrari, Pierangela Samarati and Elisa Bertino
(Universita' di Milano) and Sushil Jajodia (George Mason

University)

Automated Analysis of Cryptographic Protocols

J. Mitchell, M. Mitchell, and U. Stern (Stanford University)

1:30-3:00 Intrusion Detection and Beyond

How to Systematically Classify Computer Security Intrusions

Ulf Lindqvist and Erland Jonsson (Chalmers University of Technology, Sweden)

Surviving Information Warfare Attacks on Databases

Paul Ammann and Sushil Jajodia (George Mason University),
Catherine D. McCollum and Barbara T. Blaustein (MITRE)

Execution Monitoring of Security-Critical Programs in a
Distributed System: A Specification-based Approach

Calvin Ko (Trusted Information Systems), Manfred
Ruschitzka

and Karl Levitt (University of California Davis)

Catalytic Inference Analysis: Detecting Inference Threats
due to

Knowledge Discovery

John Hale and Sujeet Shenoi (University of Tulsa)

3:30-5:00 5-Minute talks on breaking research results

5:00-6:00 Meeting, IEEE Technical Committee on Security and
Privacy

Wednesday May 7, 1997

9:00-10:30

Panel: Security in Innovative New Operating Systems

Moderator: Cynthia E. Irvine (Naval Postgraduate School)

Panel Members: Robert Grimm, Spin Project (University of
Washington)

Frans Kaashoek, Exokernel Project

(Massachusetts Institute of
Technology)

Jay Lepreau, Flux Project (University of Utah)

George Necula, Fox Project (Carnegie Mellon
University)

Larry Peterson, Scout Project (University of
Arizona)

11:00-12:00 System Vulnerabilities

Analysis of a Denial of Service Attack on TCP

Christoph L. Schuba, Ivan V. Krsuland, Markus G. Kuhn,
Eugene H. Spafford, Aurobindo Sundaram and Diego Zambon
(Purdue University)

Deniable Password Snatching: On the Possibility of Evasive
Electronic Espionage

A. Young and M. Yung (Columbia University)

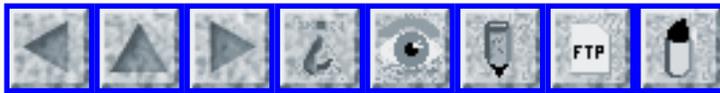
Number Theoretic Attacks On Secure Password Schemes

Sarvar Patel (Bellcore)

12:00-12:15 Final Remarks

[Truncated for RISKS. Registration form, hotel information,
etc., at

<http://www.itd.nrl.navy.mil/ITD/5540/ieee/cipher/SP97pgmandreg.html> . 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 18: Issue 94

Thursday 27 March 1997

Contents

- [Crackers Obtained Gulf War Military Secrets](#)
[Edupage](#)
- [Clinton Administration Pushing New Encryption Legislation](#)
[Edupage](#)
- [Thieves steal license machines](#)
[Gary Grossoehme](#)
- [Jail release: Just the Fax, Ma'am.](#)
[David Kennedy](#)
- [Traffic signals, red-runners & all-greens](#)
[J. DeBert](#)
- [UK Banks clearing system salary payment problems](#)
[Lord Wodehouse](#)
- [Sweden may offer constitutional protection to Internet publications](#)
[Martin Minow](#)
- [Liability risk in Web Frames](#)
[David Kennedy](#)
- [Hungary's State-Run ISP Compromised](#)
[David Kennedy](#)
- [Warning to MSIE users](#)
[Andre Hallam](#)

- [Risks of automatic spam blockers](#)
[Prentiss Riddle](#)
 - [Catastrophic Y2K risk](#)
[Joel Garry](#)
 - [Year 2000 costs -- they're large](#)
[Martin Minow](#)
 - [Re: Splendour of the Seas not so Splendid](#)
[Martin Ewing](#)
[Jeremy Anderson](#)
 - [Bad variable names in programs](#)
[Randy Holcomb](#)
 - [USENET control messages as worm transport](#)
[Steve Kilbane](#)
 - [Re: Bank cannot believe it made a mistake!](#)
[Mark Brukhartz](#)
 - [Re: Risks of random-number servers](#)
[Jeff Nelson](#)
[Przemek Klosowski](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✶ Crackers Obtained Gulf War Military Secrets (Edupage)

Edupage Editors <educom@elanor.oit.unc.edu>

Tue, 25 Mar 1997 13:06:41 -0500

During the Gulf War, computer vandals working from Eindhoven in the Netherlands cracked into U.S. government computers at 34 military sites to steal information about troop movements, missile capabilities, and other secret information; they then offered it to the Iraqis, but the Iraqis rejected it because they considered the information a hoax. Dr. Eugene Schultz, former head of computer security at the U.S. Department of Energy,

has told the British Broadcasting Company: "We realized that these files should not have been stored on Internet-capable machines. They related to our military systems, they related to Operation Desert Shield at the time, and later Operation Desert Storm. This was a huge mistake." (*London Telegraph*, 23 Mar 1997; Edupage, 25 Mar 1997)

⚡ Clinton Administration Pushing New Encryption Legislation (Edupage)

Edupage Editors <educom@elanor.oit.unc.edu>
Tue, 25 Mar 1997 13:06:41 -0500

The Clinton administration will introduce more legislation on encryption technology export, in addition to the three bills already pending in Congress. The latest effort seeks to help develop an electronic key management infrastructure that would allow U.S. users to employ any encryption they want, and would, among other provisions, spell out the legal circumstances for handing over keys to law enforcement officials. The other bills pending are: the Security and Freedom Through Encryption Act, the Promotion of Commerce Online in the Digital Era bill, and the Encrypted Communications Privacy Act. (InfoWorld Electric 21 Mar 1997; Edupage, 25 Mar 1997)

⚡ Thieves steal license machines

<GaryG4430@aol.com>

Tue, 25 Mar 1997 16:39:50 -0500 (EST)

Excuse me Sir, but would you watch my Golden Goose while I go get a cup of coffee?

Published in the **Portland Oregonian**, 25 Mar 1997, p.2, Around the Nation:

Thieves steal license machines

MIAMI - Last year, Florida bought computers to make driver's licenses that are virtually impossible to counterfeit. But brazen South Florida thieves have been stealing the computers, sometimes later returning to the scene to pick up accessories. In seven burglaries at five virtually unprotected driver's license offices from Key Largo to Okeechobee, crooks have gathered the \$15,000 computers, software and supplies for five complete systems -everything they would need to crank out the state's new high-tech, counterfeit-resistant licenses.

Yup, only our high-tech systems can make our high-security, tamperproof, extremely valuable documents. And you can't just buy one of these system just anywhere...

Gary Grossoehme, Oregon Electronics

[Also commented on by Bob_Frankston@frankston.com, who notes that if the new licenses are considered "foolproof", it only increases their value! PGN]

✶ Jail release: Just the Fax, Ma'am.

David Kennedy <76702.3557@compuserve.com>

Wed, 26 Mar 1997 16:51:47 -0500

Gregory Williamson was released from jail after his girlfriend Kim Starke faxed to jail officials a bogus letter supposedly from the Pennsylvania Governor's office, ordering his release. He was subsequently recaptured after he tried the same technique to get his former cellmate released, sending a fax that appeared to be from Florida Governor Lawton Chiles' office -- someone had bothered to check with Chiles' office. Starke formerly worked for a printing company, and investigators found computers and disks containing official seals for various state offices in her apartment. [Source: AP US & World 26 Mar 1997, Associated Press via CompuServe's Executive News Service, PGN Abstracting]

[DMK: Corel Draw 3, I wonder?]

[For newer RISKS readers, we note that jail spoofing is of course old hat.

William Londono (an alleged cocaine dealer) was released from Los Angeles

County jail in 1987 based on a bogus e-mail message, and Jean Paul Barrett

(a convicted forger) was released from a Tucson jail on the basis of a

forged fax. Earlier, a Santa Clara inmate had gotten access to the prison

computer and simply changed his own release date. PGN]

⚡ Traffic signals, red-runners & all-greens

"J. DeBert" <onymouse@hypatia.com>

Tue, 25 Mar 1997 22:37:06 -0800

I understand, from discussions with public works departments and from glancing views of the insides of controllers, that traffic signals are controlled by software, now.

A recent accident in San Francisco, in which both drivers and witnesses state they they had green lights caused me to remember some instances where I have seen modern signals go all green. (These were all stand-alone signals with no remote controls at all.)

This is obviously a serious danger to traffic, if it occurs at all. It is made worse because no one seems to believe that it is possible. I have talked to public works people and police, who all have told me that it is impossible. Sure, it quite likely is, for old-style timer and stepper relay controlled signals, but what about the new types?

Has anyone else seen signals go all green?

⚡ UK Banks clearing system salary payment problems

Lord Wodehouse <w0400@ggr.co.uk>

Thu, 27 Mar 1997 11:21:19 +0000 (GMT)

As you may have read, there was a problem with the banks

automatic clearing system earlier this week, and records for salary payment in the UK did not all get processed in time. With Easter this weekend, Good Friday a bank holiday and also Easter Monday, people whose salary was not paid, would find that the ATMs might not allow them money, because their accounts were out of funds. With two extra days when banks are closed making a period of four consecutive days, customers could well be placed in a difficult position.

I checked with my bank today, once via the telephone banking service, once in the branch and once via an ATM. The first check showed no money, the second and third showed GW had paid the money and I would not be penniless over Easter, on account of the bank clearing problems in the press today.

So everyone else in GW should be OK, but while using the ATM to query another account, it failed to make the transaction. I can only assume that the extra traffic levels because of the newspaper comment are resulting in overloads at the banks ATM computer centres.

So we have at least two problems here. The first is the failure to process all the records through the clearing system in time. The exact reason has not been given as yet. The second problem is the long "weekend" and the impact on customers. Thirdly the press coverage now increasing the load on the ATM system, and you have a very interesting situation. One simple failure causes a series of consequences, which may trigger further failures,

a domino effect.

Now the press are saying that the banks won't charge for people overdrawn as a result. I guess that will be quite taxing for people to sort that out after the event. Even if as it has been said that only a small percentage of the transfers were not completed, it certainly is already having a wide impact. At least one of the TV News desks were trying to speak to "a bank" and not getting through this morning. so BT will finding its network is having extra loadings in unusual patterns.

Of course the clocks go forward in the UK this weekend too ... on some computers, but we know the problems that often presents.

... and you think that the y2k problem is not really one ...

Advanced Technology & Informatics, Glaxo Wellcome Medicines
Research Centre
+44 (0)1438 76 3222 lordjohn@dial.pipex.com lordjohn@lordjohn.
demon.co.uk

✶ Sweden may offer constitutional protection to Internet publications

Martin Minow <minow@apple.com>
Tue, 25 Mar 1997 18:37:46 -0800

An article in the Swedish newspaper, Svenska Dagbladet http://www.svd.se/svd/ettan/ettan_97-03-22/privatpersons.html describes proposed legislation that, if passed, would offer constitutional "Freedom of Speech," protection to Internet publications, equivalent to

those granted to traditional paper publications. (Swedish constitutional protections are generally, but not totally, comparable to American practice -- and I'm not qualified to discuss this in detail.)

The "Media Committee" [the article wasn't clear as to whether this is a parliamentary committee or a non-governmental source] does not believe that the Internet itself should be covered by constitutional protection, due to the inability to maintain the principal of "ansvarig utgivare" [responsible editor -- a known individual who has legal responsibility for what is written in the publication]. On the other hand, this does not mean that the Internet is totally beyond the law as, for example, threats against national groups can be prosecuted under existing criminal law.

There is one interesting limitation in the legislative proposal: that an Internet publication would receive constitutional protection by 'requesting an "utgivnings bevis" [publication manifest] from the Radio and TV Commission.' The limitation is that the reader shall not be permitted to modify the material. This would appear to exclude unedited chat rooms, list servers, or unmoderated news groups. Anonymity (on the part of the editor) would also be forbidden.

[Note: this is more of a summary than a direct translation. Svenska Dagbladet is a major national newspaper. Articles on their web page generally disappear after a week, but can be retrieved for a fee. There are

several terms of art, such as "ansvarig utgivare" that have very specific meaning in Swedish law, and my translations should not be trusted.

The Swedish "grundlag" [constitution] is the basis for the Swedish legal system. Of interest here are (using American terms) the freedom of the press and freedom of expression laws. These grant citizens the right to publish without prior governmental hindrance. This freedom does not permit high treason, threat against national groups, illegal description of violence, and slander.]

Martin Minow minow@apple.com

⚡ Liability risk in Web Frames

David Kennedy <76702.3557@compuserve.com>

Tue, 25 Mar 1997 18:23:09 -0500

Excerpted from:

EFFector Vol. 10, No. 04 Mar. 17, 1997

editor@eff.org

A Publication of the Electronic Frontier Foundation

ISSN

1062-9424

* Web Link Lawsuits Raise Serious Questions

Comments of the Electronic Frontier Foundation on Web Content

Linkage Lawsuits

Mar 17 1996

In an action similar to a (settled) legal threat over "inlining" of copyrighted comic strip graphics in a third party web page, a host of publishing companies have filed suit in New York City federal

district court
against a company called TotalNews. TotalNews uses the
experimental
"frames" extension to Web code to point their site's visitors to
various
news sources around the Web. CNN, Washington Post, Dow Jones,
Times Mirror
and Reuters, who have filed the suit, allege that TotalNews'
practice of
displaying the content of the various companies' news sites
within a "frame"
with TotalNews' banner ads, is a violation of the companies'
rights. [...]

Dave Kennedy [CISSP] Research Team Chief, National Computer
Security Assoc.

[Recall the Shetland Times suit, [RISKS-18.64](#) and 78. PGN]

⚡ Hungary's State-Run ISP Compromised

David Kennedy <76702.3557@compuserve.com>
Wed, 26 Mar 1997 00:22:29 -0500

Courtesy of the COMTEX Newswire via CompuServe's Executive News
Service:

COMTEX Newswire 25 Mar 1997

****Hungary's Matav Admits Internet ID/Password Leak

> BUDAPEST, HUNGARY, 1997 MAR 25 (Newsbytes) -- By Sylvia
Dennis. Matav,
> the former state telco in Hungary, has been forced to admit
that security
> in its Internet division is not all it could be. Following an
anonymous
> post to several Hungarian mailing lists, the Internet service
provider
> (ISP) has admitted that around 1,200 IDs and passwords for the

MatavNet

> may have fallen into the wrong hands.

> The saga started last week when an anonymous set of messages started

> appearing in the Hungarian Usenet newsgroups, claiming that the poster had

> obtained a list of MatavNet IDs and passwords, and that the files had been

> leaked because of the ISP's security failures.

1200 subscribers were signed up for accounts in the second quarter of 1996

and were given accounts where the password was their billing ID number. The

ISP published the ID numbers a "few months ago ... with predictable

results." The ISP published the list to alert users to change their

passwords (DMK:?!?).

> The incident has similarities to a security problem caused in the

> mid-1980s by Telecom Gold, British Telecom's e-mail company, Newsbytes

> notes. Telecom Gold officials released 100's of IDs in the ICL001 to

> ICL999 ID group to ICL Computers, but allocated the IDs as passwords as

> well, and told ICL staff what they had done.

Hackers responded predictably within days. It took weeks to discover the

problem, resulting in several thousand pounds lost.

Ameritech and Deutsche Telekom are major investors in MatavNet.

> MatavNet's Web pages are at <http://www.datanet.hu> .

Warning to MSIE users

Andre Hallam <***agh@netcom.ca>

Thu, 27 Mar 1997 05:21:12 GMT

You've probably heard about the infamous bug that lets people run code on your system. Well, really, it's quite a lot worse than that, and Microsoft is not telling you. Why aren't they telling you? I don't know.

It is possible for someone to steal any file on your system. This includes your password files, your INI files - anything at all.

I have informed Microsoft about this serious hole, and sent them instructions on how to duplicate it, but this has not caused them to escalate their warnings in any way. I think they're hoping nobody finds out about it.

(Remove asterisks from my address if you would like to reply. Andre)

[Ah, yes, by all means, avoid the aste-RISKS of being spammed! And if you have questions, please direct them to Andre, cc RISKS. PGN]

⚡ Risks of automatic spam blockers

Prentiss Riddle <riddle@is.rice.edu>

Wed, 26 Mar 1997 09:25:38 -0600 (CST)

Forwarded from Edupage, 25 March 1997:

| SPAM BLOCK

| A California software engineer [Ron Guilmette] takes the annoyance

| caused by unsolicited e-mail messages seriously, and has developed an

| anti-spam weapon he plans to unveil next month. Dead Bolt

allows

| online users to share their "blacklists" of spam purveyors so that they

| can more effectively filter offending e-mail. "The problem now is that

| everyone who is filtering is keeping their own blacklists and they're

| not working together to tie their lists together in a meaningful way,"

| says Dead Bolt's creator. "What I hope my package will do is allow

| people to work together over the Net and filter all this stuff out and

| finally put these people out of business....The problem is that it

| costs the sender virtually zero dollars to send out a million messages,

| and even if the response rate is minuscule by all standards -- say .001

| percent -- they've made money. So from an economic selfish point of

| view, it's in their interest to annoy the other 99.99 percent of the

| people." (Miami Herald 24 Mar 97)

The full Miami Herald article is available at:

<http://www.herald.com/archive/cyber/techdocs/056735.htm>

Some of the risks of automatic spam filtering which Deadbolt will have

to overcome in order to be successful include:

-- The risk of false and malicious blacklisting of non-spammers.

-- The risk of harm to innocent bystanders who happen to share hostnames, ISPs, or other characteristics with targeted spammers.

-- The possibility that spam messages will avoid detection by varying return addresses and other signatures in each copy of

a message.

I find the first two particularly troubling -- were an imperfect spam filtering system in wide use, then triggering it against an innocent party could become a handy form of denial-of-service attack.

Published details of Deadbolt are sketchy, but a Deja News or Alta Vista search of Usenet for "Ron Guilmette" reveals some of its designer's thinking on the subject. So far, I don't see enough to convince me that he will be successful.

Prentiss Riddle riddle@rice.edu

✶ Catastrophic Y2K risk

Joel Garry <joelga@amber.rossinc.com>

Thu, 27 Mar 1997 06:14:42 -0800

The news is awash with stories of the Rancho Santa Fe (by some measures, the most affluent community in the US) apparent religious-cult mass suicide yesterday. [39 dead.] The reports mention that 4 or 5 of the victims were web programmers. Beyond the obvious Y2K risk of losing your programmers to Millennium cults, this may bring to the public consciousness the risk of a doomsday cult seeking to destroy the Net, which of course leads to the risk that the public may become paranoid about that risk. Paranoid nontechnical people may be a worse risk than malicious technical people.

Joel Garry joelga@rossinc.com

✶ Year 2000 costs -- they're large

Martin Minow <minow@apple.com>

Thu, 27 Mar 1997 08:59:27 -0800

In an article in the Swedish newspaper, Svenska Dagbladet, <http://www.svd.se/svd/ettan/dagens/tusenarsskiftet.html> Jan Freese, the general director of the Swedish PTT, estimated that that the total national cost [not just the PTT] for fixing the year 2000 problem will be roughly SKR 30,000 (\$4,000) per Swedish citizen. He made his estimate based on a report by Capers Jones, "Global economic impact of the year 2,000 software software problem." That report estimates the total cost of fixing the problem as roughly comparable to the total Swedish GNP for the entire 1980's.

One paragraph from a long, interesting, article, quickly summarized.

The Capers Jones report (from Software Productivity Research of Burlington, Massachusetts) might be worth pursuing. Their web page is at <http://www.spr.com/> and Capers Jones report is at <http://www.spr.com/library/y2k00.htm> (follow the link to the current version).

Martin Minow minow@apple.com

✶ Re: Splendour of the Seas not so Splendid (Kabay, [RISKS-](#)

18.93)

Martin Ewing <martin.ewing@yale.edu>

Tue, 25 Mar 1997 09:46:51 -0500

> [I suppose it might add to the hypothetical risks if the ship
were to
> cross the equator for the first time precisely at the Y2K
midnight! PGN]

The most dangerous spot might be on the equator and on the
international
dateline at Y2K +/- 1 day.

Martin Ewing, Science & Engineering Computing Facility, Yale
University

73 de AA6E martin.ewing@yale.edu, 203-432-4243, <http://www.yale.edu/secf/>

[Also noted by Jason Yanowitz <yanowitz@jimi.hmm.com>. I
should also have

mentioned the international date line, but I was thinking
primarily of

the F-16 whose software simulation detected the bug that had
caused the

virtual plane to turn upside down when crossing the equator,
because a

programmer had forgotten the relevance of the latitude sign.
PGN]

✉ Re: Splendour of the Seas not so Splendid (Kabay, [RISKS-18.93](#))

Jeremy Anderson <jsamail@transend.com.tw>

Tue, 25 Mar 1997 13:37:45 +0800 (CST)

This is an amusing article. Having once worked in the marine
industry, I

have heard stories like this over and over. The level of computerization on many working boats continues to be low (outside of radar, GPS and the like) because of the number of stories like this that get told and retold.

The technical problems of shipboard systems are fairly straightforward: you are dealing with mission-critical systems which are subject to heat, humidity, occasional quantities of salt water, inept workers and various permutations thereof (let me tell you about the one where a high-speed fish filleting line's automation system had the control door left open during the daily cleaning, and was subjected to 60PSI salt water). These sort of problems can be engineered around with backup systems, industrial-grade computers, and hosing down inept helpmeat with 60PSI salt water.

The more common problems tend to be the same as those encountered on land. The non-technical owners of boats do not understand the intricacies of fault-tolerant systems or their associated costs. They understand that these systems are many times more expensive than systems without environmental protection or backups, and are very suspicious of suppliers screwing them (if you dealt with waterfront types on a regular basis, you would be too).

... Thus none-too-splendid seas.

✶ Bad variable names in programs (re: Kaiser, [RISKS-18.92](#))

"Randy Holcomb" <randyh@ibm.net>

Tue, 25 Mar 1997 22:13:50 -0600

Bad variable names and poor documentation are a problem in ANY computer language, and their risks have been well known for quite a while.

It should not be forgotten that some compiler implementations of yesteryear had limits on how many characters identifier names could be; I recall from some 20 years ago on the Honeywell Model 58 that had 2 different COBOL compilers- a 'MiniCOBOL' compiler which had 5 phases (and only recognized 4 characters in variable names) to the ANS 68 COBOL compiler, which used 21 phases - and up to six times longer to compile the same code for the same function.

Many of the commercial packages today that I have seen and worked with (those that are delivered with source-good luck with OCO applications) do have meaningful identifier names and adequate documentation-but as with anything else, its value will be variable to the programmer assigned.

Randy Holcomb (randyh@ibm.net)

⚡ USENET control messages as worm transport

<Steve_Kilbane@cegelecproj.co.uk>

Tue, 25 Mar 1997 09:33:04 GMT

I haven't seen any comments on this in recent RISKS articles, so

I thought
I'd mention it. On 15 Mar 1997, David Lawrence warned in news.
admin.announce
that control messages had been posted in his name which
exploited a bug in
versions of innd prior to 1.5.1. The deviant messages mailed
passwd and
inetd configuration information to a number of addresses. CERT
has issued an
advisory (CA-97.08.innd) concerning this.

What I find interesting about this is the comparison between
this attack and
RTM's 1988 Internet Worm. The original worm expended a lot of
effort to move
from one machine to another, propagating itself. The design of
the USENET
control system does exactly that. Usenet control messages *are*
worms,
performing a usually benign task.

For more information, see:

ftp://info.cert.org/pub/cert_advisories/CA-97.08.innd. I'd give
a reference
to David Lawrence's message too, but our news system has
undergone a sudden
complete re-install, and we no longer have the article
available. :-)

steve

✶ Re: Bank cannot believe it made a mistake! ([RISKS-18.92](#))

Mark Brukhartz <mark_brukhartz@il.us.swissbank.com>

Wed, 26 Mar 1997 13:29:03 -0600

I recall a similar story in the news. The recipient of an
``impossible''
erroneous deposit withdrew it as a bank cashiers' check and

locked it in his safe deposit box at the same bank. He demanded and received a public apology in exchange for the return of the check.

About 20 years ago, a bank gave me a \$32,000 check in exchange for a \$320 withdrawal. The teller erred in keying the amount into the imprinter. The bank teller supervisor agreed that I could have cashed it (with a raised eyebrow, no doubt) at the other local bank where I held an account. Since then, I've noticed that the banks have imposed a one-day hold on cashiers' checks. That is insufficient for them to actually receive the funds, but is probably adequate for a few basic fraud safeguards.

✉ **Re: Risks of random-number servers (Re: Zaba, [RISKS-18.93](#))**

Jeff Nelson <jnelson@dialogosweb.com>
Wed, 26 Mar 1997 15:54:56 -0500

In [RISKS-18.93](#), Stefak Zaba writes that random-number servers on the Internet should not just PGP-sign but also encrypt their data, if such data is to be used for trusted applications.

Numerous attacks are known against many different cryptographic algorithms, including RSA, which allow statistical information to be gained about certain bits or the combination of certain bits in the plaintext message.

In order to prevent any of this statistical information about the random numbers from being stolen en route to the consumer, the consumer

would have
to use only "hard core" bits of the message. That is, bits
which have been
proven such that gaining any statistical information about them
is
equivalent to breaking the cryptographic algorithm.

This situations demonstrates the risks inherent in trusting a
tool/technology which has proven excellent at solving one
problem to solve
other related problems, when the tool may or may not actually
have the
required properties.

Ref. Advances in cryptology, {EUROCRYPT} '95: Kouichi Sakurai
and Hiroki Shizuya. Universal hash functions and hard core bits.

Jeff Nelson <corba@acm.org> See also <http://www.dialogosweb.com>

✉ Re: Risks of random-number servers (Re: Rescorla, [RISKS-18.91](#))

Przemek Klosowski <przemek@rrdjazz.nist.gov>
26 Mar 1997 13:08:09 -0500

I wonder how many people looked into the random number generator
incorporated into Linux kernel. It tallies the random events
happening in a
running system (various interrupt intervals---keystroke, disk
access, etc),
and constructs random bits based on them. It is written to
block if you try
to read too many bits ('entropy pool' emptied out).

I haven't looked into the implementation, but I'm sure there are
people on
this list who can pass a judgement on the strengths/weaknesses
of this
approach.

przemek klosowski, Reactor Division, National Institute of
Standards and
Technology Gaithersburg, MD 20899 1-301-975-6249 <przemek@nist.
gov>



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 18: Issue 95

Friday 28 March 1997

Contents

- [DTI proposals on key escrow](#)
[Ross Anderson](#)
- [RISKS of analogy: Elections Canada and the Net](#)
[Mich Kabay](#)
- [SSL Browser Vulnerability Discovered](#)
[David Kennedy](#)
- [JavaScript attack through MIME attachments](#)
[Ted Wong](#)
- [Generating randomness](#)
[Paul C. Kocher](#)
- [Computers in California Senate](#)
[Keith Price](#)
- [DC traffic-light synchronization problem](#)
[David Pipes](#)
- [Re: all-ways green lights](#)
[Robert Miller via J. DeBert](#)
[Sean Ercanbrack](#)
[Barak Pearlmutter](#)
- [God, the sweepstakes winner](#)
[Kevin A. Hogan](#)

- [Re: Crackers Obtained Gulf War Military Secrets](#)
[Fred Cohen](#)
 - [Re: Y2K: revenge of originality](#)
[Harlan Rosenthal](#)
 - [Y2K costs](#)
[Richard Schroepel](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ DTI proposals on key escrow

Ross Anderson <rja14@cl.cam.ac.uk>
21 Mar 1997 10:11:57 GMT

The British government's Department of Trade and Industry has sneaked out proposals on licensing encryption services. Their effect will be to ban PGP and much more besides.

I have put a copy on <http://www.cl.cam.ac.uk/users/rja14/dti.html> as their own web server appears to be conveniently down.

Licensing will be mandatory:

We intend that it will be a criminal offence for a body to offer or provide licensable encryption services to the UK public without a valid licence

The scope of licensing is broad:

Public will be defined to cover any natural or legal person in the UK.

Encryption services is meant to encompass any service, whether provided free or not, which involves any or all of the following

cryptographic

functionality - key management, key recovery, key certification, key

storage, message integrity (through the use of digital signatures) key

generation, time stamping, or key revocation services (whether for

integrity or confidentiality), which are offered in a manner which

allows a client to determine a choice of cryptographic key or allows

the client a choice of recipient/s.

Total official discretion is retained:

The legislation will provide that bodies wishing to offer or provide

encryption services to the public in the UK will be required to obtain

a licence. The legislation will give the Secretary of State discretion

to determine appropriate licence conditions.

The licence conditions imply that only large organisations will be able to

get licences: small organisations will have to use large ones to manage

their keys (this was the policy outlined last June by a DTI spokesman). The

main licence condition is of course that keys must be escrowed, and

delivered on demand to a central repository within one hour. The mere

delivery of decrypted plaintext is not acceptable except perhaps from TTPs

overseas under international agreements.

The effect of all this appears to be:

1. PGP servers will be outlawed; it will be an offence for me to sign your

pgp key, for you to sign mine, and for anybody to put my existing signed

PGP key in a foreign (unlicensed) directory

2. Countries that won't escrow, such as Holland and Denmark, will be cut out

of the Superhighway economy. You won't even be able to send signed

medical records back and forth (let alone encrypted ones)

3. You can forget about building distributed secure systems, as even

relatively primitive products such as Kerberos would need to have their

keys managed by a licensed TTP. This is clearly impractical. (The paper

does say that purely intra-company key management is OK but licensing is

required whenever there is any interaction with the outside world, which

presumably catches mail, web and so on.)

There are let-outs for banks and Rupert Murdoch:

Encryption services as an integral part of another service (such as in

the scrambling of pay TV programmes or the authentication of credit

cards) are also excluded from this legislation.

However, there are no let-outs for services providing only authenticity and

nonrepudiation (as opposed to confidentiality) services. This is a point

that has been raised repeatedly by doctors, lawyers and others - giving a

police officer the power to inspect my medical records might just conceivably help him build a case against me, but giving him the power to

forge prescriptions and legal contracts appears a recipe for disaster. The

scope for fraud and corruption will be immense.

Yet the government continues to insist on control of, and access to, signing

keys as well as decryption keys. This shows that the real concern is not really law enforcement at all, but national intelligence.

Finally, there's an opportunity to write in and protest:

The Government invites comments on this paper until 30 May 1997

Though if the recent 'consultation' about the recent 'government direct' programme is anything to go by, negative comments will simply be ignored.

Meanwhile, GCHQ is pressing ahead with the implementation of an escrow protocol (see <http://www.cs.berkeley.edu/~daw/GCHQ/casm.htm>) that is broken (see <http://www.cl.cam.ac.uk/ftp/users/rja14/euroclipper.ps.gz>).

In Grey's words, 'All over Europe, the lights are going out'

Ross

⚡ RISKS of analogy: Elections Canada and the Net

"Mich Kabay [NCSA]" <Mich_Kabay@compuserve.com>

Thu, 27 Mar 1997 12:01:09 -0500

In the **Globe&Mail**, 27 Mar 1997, p. A6, their Applied Science Reporter tells another story of how governments are fearful of uncontrolled human communications.

[MK: Some background: Canada, like the US and Russia, is so wide that many people in the Western areas must vote after vote-counting has begun in Eastern regions. Election officials have long been concerned

about the effects of releasing late public-opinion polls and also preliminary vote-counts from the East; they claim (I have never seen any reference to evidence, but this is not my field of expertise) that knowing these data influences the vote by discouraging votes or by changing them. There are therefore strict rules in Canada on what the news media may say in the run-up to the actual vote.]

> Elections Canada scrambling to plug cyberspace loophole:
> Officials hope to bring election law to the wilds of the Internet.
> by Mary Gooderham
> Elections Canada is scrambling to jam its finger in the electronic dike.
>
> Officials have decided that the Internet will face the same rules as other news media when it comes to disseminating public opinion polls within 48 hours of election day and releasing vote results early on election night.

The reporter makes the following key points:

* The Canada Elections Act forbids premature "publishing" voting results by any means.

* The 48-hour blackout on advertising by political parties does not apply to the Net.

* John Enright, a spokesperson for Elections Canada, said that the Office would investigate and prosecute any breach of the Act, but admitted that actually catching violators who use the Net is "virtually impossible."

* Professor John Courtney (political science, University of Saskatchewan) raised the question of whether the Office would try to forbid electronic mail from residents of the east to residents of the west.

[Comments by MK:

So the bureaucrats are trying to push back the tide again. I expect this sort of nonsense from authoritarians in the PRC, Burma, and so on; it's distressing to see people in Canada uttering such rubbish. What's next, an attempt to stop people in Newfoundland from phoning their friends in British Columbia to safeguard the sacred innocence of Westerners?

The problem here is that the Elections Canada officials are stuck in a primitive analogy. Change their view of the Net as a medium for "publishing" to a view that does not try to force the models of the past on the current reality and the problem disappears. The Net is not merely like newspapers, nor merely like a bookstore, nor merely like a fax machine, nor merely like a billboard. These folks need a dose of general semantics: the symbol is not the thing. As Professor Courtney is quoted as saying in the article, "The question is: Does it affect how you vote or whether you vote?" The fundamental issue is not technological: it is whether a government has any business at all controlling what information individuals willingly seek out.]

Mich M.E. Kabay, PhD, CISSP (Kirkland, QC), Director of Education
National Computer Security Association (Carlisle, PA) <http://www.ncsa.com>

SSL Browser Vulnerability Discovered

David Kennedy <76702.3557@compuserve.com>

Fri, 28 Mar 1997 00:41:42 -0500

<http://www.zdnet.com:80/intweek/daily/970327x.html>

Inter@ctive Week

March 27, 1997

New Browser Security Flaw Discovered

By Will Rodger

> Internet browsers set up to protect users' credit card numbers from theft

> are unwittingly handing out those numbers to untold numbers of other Web

> sites as visitors follow links from those sites to other, insecure ones,

> officials from Netscape Communications Corp. and Microsoft Corp. confirmed

> Wednesday. The hole, though thus far unexploited, now appears to be the

> most serious flaw yet discovered in the way Internet browsers handle

> confidential information over the Internet.

> "The place people will crack it is not the places people worry about

> security but the ones they don't," said Daniel Klein, a Pittsburgh-based

> consultant who discovered the hole earlier this month. "This is a big

> hole."

:: Both MS and Netscape say patches may take weeks to release.

> "This is a serious problem," said Eugene Spafford, director of the

> Computer Operations, Audit, and Security Technology program at
Purdue
> University in Indiana. "This isn't a good response because
it's not clear
> how many other people are going to be impacted by it."
>
> But Steven Bellovin, a computer security researcher at AT&T
Corp. labs,
> warned Microsoft and Netscape could find the problem difficult
to
> surmount. "The reality of software engineering making a quick
and dirty
> fix to a large program is likely to cause more problems than
it fixes," he
> said. "First you have to decide what the fix is." [...]
>
> But if a visitor who has just filled out a secure form then
clicks on a
> highlighted link to another Web site, all bets may be off. The
information
> that Web user typed in securely suddenly gets transferred to
the logs of
> the next machine, credit card numbers and all.

:: Server-side remedies include referring visitors to an in-
house dummy
page to "wipe the browser's feet," or use the POST command
instead of GET.

> Users finally, can protect themselves by typing in Internet
addresses
> manually instead of using links from "secure" pages.

Dave Kennedy [CISSP] Research Team Chief, National Computer
Security Assoc.

[Starkly excerpted by Dave. PGN]

JavaScript attack through MIME attachments

Ted Wong <tmw5@cornell.edu>

Fri, 21 Mar 1997 12:36:03 -0500

Netscape's JavaScript includes a command, `window.open(...)`, for spawning a new browser window from within a web page. This feature, when combined with the fact the Netscape (by default) will display text/html MIME attachments as regular web pages, can be used to create a denial-of-service attack.

A particularly obnoxious individual (let's call him A. User), created a web page containing JavaScript code to spawn an infinite number of new browser windows. Someone visiting this page will immediately see windows popping up all over the screen, with no way to gracefully exit Netscape; it stops responding to keyboard or mouse input while tied up executing the spawn loop.

Now, another user (B. User) posted a message to comp.misc, warning people not to visit the offending web page. The problem is that B. User included the document source for the page as a text/html MIME attachment. Anyone viewing the message with the Netscape news reader will immediately execute the spawner. The only way (for me, at least) to stop the errant JavaScript code was to (Unix) kill Netscape.

This touches upon RISKS discussed here before, particularly those that involve shipping software with minimal security set as the default. One can imagine a scenario where some malcontent spams several mail addresses with this attachment, with a good chance that an unlucky recipient

will be using
the Netscape mail viewer in its default JavaScript-enabled mode.
This attack
mechanism goes some way towards achieving what the "Good Times"
e-mail
claimed to do in word, if not in deed.

I'm now running with JavaScript disabled. The document source is
off of
A. User's home page at <<http://www.olywa.net/jwalker/j0ck.htm>> -
remember to
view it with JavaScript turned off!

Ted Wong <tmw5@cornell.edu>
Information Technology Section, Mann Library, Cornell University

🔥 Generating randomness (re: Klosowski, [RISKS-18.94](#))

Paul C. Kocher <pck@netcom.com>
Fri, 28 Mar 1997 01:04:13 -0800

Was: Risks of random-number servers

The notion that the random pool used in a cryptographically
secure PRNG
"runs out" of entropy is not one I agree with. With a properly-
seeded
cryptographic PRNG, there shouldn't be any limit to the amount
of random
material you can produce (unless the crypto function starts
failing).

A secure PRNG is simply a good stream cipher. Although it's
possible to use
a one time pad and use as much input entropy as output material,
this would
be very cumbersome and isn't at all needed for encryption or a
PRNG.
Instead, the design goal to to make sure that that someone who

doesn't know
the entire key or PRNG seed cannot distinguish the output from a
truly
random sequence of equal length with a probability significantly
better than
guessing randomly. In other words, a well-seeded cryptographic
PRNG should
be perfect. (In contrast, PRNGs based on physical phenomena
often produce
output with biases and other major imperfections and really
should only be
used for seeding cryptographic PRNGs)

Not all of the high-speed stream ciphers in use today meet the
requirements
for being a good PRNG, so care has to be taken when designing or
selecting
PRNG algorithms. One also has to make sure to use adequate key
lengths
(e.g., a single-DES PRNG shouldn't be used to generate triple-
DES keys and
the PRNG state needs to be big enough!), seed update functions
must remix
the state completely, the PRNG must not cycle, etc. Other
things can also
go wrong -- for example, several applications have had PRNG
failures because
one of the most widely-used PRNGs has the property that seeding
with seed
block "A" followed by "B" is the same as seeding with "B" then
"A". Seeding
with a large number of low-entropy seed blocks thus produces a
PRNG state
with much less entropy than would normally be expected.

Methods for collecting initial seed data are generally platform-
specific
and sometimes cause problems in crypto products (though most
companies seem
to have learned from Netscape's lesson). There are various
approaches which
can be used for seeding, but I usually combine seed material
from three

sources: event timing data (keystroke, mouse, etc.), the user's private key (or, better, a hash/HMAC of the private key) combined with the date/time, and state saved from last time the PRNG was used. Any one of the three should be enough to thwart attacks. Throwing in additional data from a random number server wouldn't hurt, though it also doesn't help since the data isn't generated and delivered in a secure enough manner. (You also have to be careful that the random server can't be used to compromise the PRNG!)

As I mentioned before, it's usually fine to leave a PRNG alone once it's seeded, though occasionally it's useful to update the PRNG state periodically to ensure that past compromises of the state will get fixed automatically. However, in practice someone who can compromise the PRNG state can often just as easily compromise the PRNG software itself, so this is often overkill and just leads to a false sense of security.

Paul

⚡ Computers in California Senate

Keith Price <price@raycharles.usc.edu>
Thu, 27 Mar 1997 13:26:02 -0800 (PST)

Today's (Thursday, March 27, 1997) LA Times reports on the use of computers in the State Senate -- The story begins:

>Computers Bring Down Load of Trouble

> Money: After spending \$1.2 million on laptops, Senate is still
relying on
> what was to have been made obsolete--paper.
> By CARL INGRAM, Times Staff Writer
>
> SACRAMENTO--In one of his first acts as the new leader of the
Senate two
> years ago, Bill Lockyer ordered the tradition-bound chamber
into the
> high-tech age by outfitting all 40 senators with laptop
computers at their
> desks. But, after spending \$1.2 million, the Senate finds
itself relying
> on what was to have been made obsolete--paper.

And goes on to report that at most 10 senators actually use the
laptops. The
cost was in 2 waves -- the first system no one liked (\$750K),
and the second
one (\$508K) with "cartoonish" graphics and a touch screen
buttons.

Complaints include, too hard to read (especially text of bills),
and too
slow when really needed (everyone needs it at the same time).

It also reports the Assembly members are far more accepting of
the simpler
system installed there.

(Available at least today online:
<http://www.latimes.com/HOME/NEWS/STATE/t000027706.html>)

Keith Price price@usc.edu

⚡ DC traffic-light synchronization problem

David Pipes - Sun Education <David.Pipes@East.Sun.COM>
Fri, 28 Mar 1997 09:56:31 -0500 (EST)

On 28 Mar 1997, a local Washington DC radio station (WTOP) reported that the traffic lights at a downtown intersection (17th and Constitution) were green in all directions at the same time. This was reported by drivers calling in on cell phones, and was apparently recurring over at least a half hour during the rush hour. This is a very dangerous situation given the number of reckless driving incidents in the region over the last few months. I have not yet heard whether any accidents occurred because of this flaw.

>From earlier reports on the system, DC uses a synchronization system that "rolls" green lights down the major streets at a rate designed to control traffic. This implies that there is an overall plan to the layout, as manual control of so many lights should be nearly impossible.

I'm very curious, given this assumption, as to how this situation occurred in the first place. I can understand that the timings could go into the wrong synchronization if they were being adjusted, but I had always thought that the default behavior in such situations should be to change all the affected lights to flashing red, which means "stop before proceeding". Are traffic light control systems built without this kind of safeguard?

David Pipes robear@access.digex.net

✉ **Re: all-ways green lights (DeBert, [RISKS-18.94](#))**

"J. DeBert" <onymouse@hypatia.com>

Thu, 27 Mar 1997 17:27:42 -0800

(I received this by e-mail in response to the item I posted to RISKS. It is posted here with the author's permission but edited slightly to improve readability.)

Date: Thu, 27 Mar 97 16:33:19

>From: "Robt. Miller" <robtmil@prolog.net>

Subject: Re: all-ways green lights (DeBert, [RISKS-18.94](#))

Last year my family and I were coming home from somewhere or other and at an intersection noticed cars going slowly, some were stopped with people looking at the lights - sure enough, they were all green. Fortunately, someone noticed it, possibly because a 7/11 type store sat catercorner[*] to the light, enabling a view of both lights at the same time. This particular intersection hosted a state road and another heavily travelled road which, needless to say, should have been more tragic than it was.

talk robtmil@cable019054.cable.eph.ptd.net

[* Robert had "caddycorner". Webster's gives "catercorner" (with "cater"

from quatre), or alternatively "kitty-corner" (presumably because "Kater"

auf deutsch = our english "cat" -- ergo, a francogerman pun in English).

The design doctrine that traffic lights must never be four-way green is

therefore presumably "caterchism". PGN]

✶ Re: all-ways green lights (DeBert, [RISKS-18.94](#))

Sean Ercanbrack <sercanbrack@juno.com>

Tue, 25 Mar 1997 22:37:06 -0800

A couple of years ago, I had an accident where a woman pulled out in front of me. I was heading home from work. My light was green, and she claimed her light had turned green also. (Note: The lights in this intersection were new and had only been installed weeks before.) There were no witnesses, so the police officer was not yet able to issue a citation--Both of us claimed to have the green light. He said he would need to get back with us when the fault was determined, probably later in the week.

Both of our cars were drivable, so we left the accident scene. The next day, I was driving home from work again along the same route and approached the intersection where the previous day's accident scene had taken place. There, in the intersection was an accident that looked exactly like the accident I had been in the day before.

I decided to pull over and ask them a few questions. Both of these accident victims claimed their lights had been green. Coincidence? I don't think so. Two different and yet identical accidents that occur at the same intersection at around the same time during the day, with all involved individuals claiming their light was green. This was a little too much for me.

I ended up calling the investigating officer and my insurance

company and
telling them about this. (All of us involved in the accidents
exchanged
phone numbers). The police said they would investigate this.
The funny
thing is that the police later denied that there was a problem
with the
lights, yet for the next few days, they had repairmen out
working on the
lights in that intersection. I have since watched those lights
carefully,
but have never seen this occurrence happen again.

✉ Re: all-ways green lights (DeBert, [RISKS-18.94](#))

"Barak Pearlmutter" <bap@cs.unm.edu>

Thu, 27 Mar 97 20:36 MST

A few years ago I learning something about actual traffic-control devices.

The engineers are acutely aware of the issue of safety in the face of

failures of both hardware and software, and the certification process in

most countries requires documentation of careful attention to these issues.

These devices are subject to very rough treatment: lightning, power spikes,

shrapnel from automobile accidents, salt water. They are designed to fail

safe: sturdy low level hardware interlocks (like relays and steppers) should

prevent any software fault, and any hardware fault outside the interlocks

themselves, from causing an unsafe configuration like all-green. Most

faults in the interlock subsystem itself should put the device into a

failsafe mode like all-blink-red.

I'd think that the most likely cause of the nightmare all-green fault would be incorrect maintenance of the device, in which maintenance workers crossed wires or disabled interlocks.

Someone from the manufacturer should have a very thorough look at the traffic control device involved in that accident in San Francisco.

Barak A. Pearlmutter <bap@cs.unm.edu>, <http://www.cs.unm.edu/~bap/>

Assistant Professor, Computer Science Dept, Univ New Mexico

[As RISKS readers have observed, there is a big difference between

"should prevent" and "do prevent". PGN]

✶ God, the sweepstakes winner

"Kevin A. Hogan" <kahogan@EECS.Berkeley.EDU>

Thu, 27 Mar 1997 10:21:44 -0800 (PST)

Yet another example of direct-mail marketers' software failing to divine the proper form of address for their intended recipient (from National Review, 24 Mar 1997, p. 5):

American Family Publishers sends Assemblies of God church in Bushnell,

Fla., a sweepstakes notice: "God, we've been searching for you." If He

wins, "what an incredible fortune there would be for God! Could you

imagine the looks you'd get from your neighbors? But don't just sit

there, God."

Kevin Hogan kahogan@EECS.Berkeley.EDU (510) 664-2533

<http://www-ucsee.EECS.Berkeley.EDU/~kahogan/>

✶ Re: Crackers Obtained Gulf War Military Secrets ([RISKS-18.94](#))

Fred Cohen <fc@ca.sandia.gov>

Thu, 27 Mar 1997 13:22:59 -0800 (PST)

It's not factually accurate. Dr. Eugene Schultz was never head of computer security at the U.S. Department of Energy - he was one of the people who started up the CIAC team at LLNL. That means he was a UC Berkeley employee. Quite a stretch if you ask me. I don't know about the rest of the story, but normally when one completely false statement appears, you can expect that everything else is likely to be tainted.

[Fred Cohen can be reached at tel:510-294-2087 fax:510-294-1225]

[The alleged Schultz quote is apparently something like 18 months old,

and Gene has maintained in the past that he was grossly misquoted -- as

I recall, he has claimed he never said that SECRET-level *classified*

information was obtained, although by inference you might suspect that

there could have been sensitive information, and that the aggregation of

the UNCLASSIFIED information could have been deemed SECRET. (Gene is

unavailable this week, so I cannot get a first-hand comment from him.)

Unfortunately, to the unwashed, all DoD computer information

seems to be

called "secret" unless it is posted to a newsgroup or available on the

Web. On the other hand, if any SECRET information had been disclosed,

that knowledge would itself most likely have been classified SECRET -- in

which case it wouldn't appear in RISKS until declassified!
PGN]

🔥 re: Y2K: revenge of originality ([RISKS-18.90,92](#))

"Rosenthal, Harlan" <rosenthh@dialogic.com>

Fri, 21 Mar 97 9:34:09 -0500

"undocumented assembler code"? The assembler is not the problem. Shoddy

practices are. I try to write assembler routines for a high-performance

realtime embedded system using meaningful data structures and commented flow

of control; I review C programs with constants named "STATE_1" and "STATE_2"

and variables with single-letter names (and I don't just mean "i" for a

loop) or names like "data". At least names like "temp" are vaguely honest.

I forgot who wrote in CACM many years ago, regarding then-new languages like

Pascal and Ada which supposedly enforced better standards, "One can write

Fortran in any language".

-Harlan Rosenthal

Y2k costs

"Richard Schroepfel" <rsc@cs.arizona.edu>

Thu, 27 Mar 1997 14:49:35 MST

Martin Minow passes along a Swedish article estimating Swedish Y2K costs at \$4000 per capita.

I find many of the estimated Y2K costs hard to believe: Is the total cost of all software ever written this large? In the US, a similar estimate would put our Y2K cost at a trillion dollars.

There is a real problem, but some people have made a business of exaggeration. A serious discussion of the costs might be warranted.

I haven't looked at the report that MMs message points to. [Life is short.

I don't read reports of flying saucers either.]

Rich Schroepfel rsc@cs.arizona.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 18: Issue 96

Monday 31 March 1997

Contents

- [END OF VOLUME 18](#)
[Peter G. Neumann](#)
- [Computer model blamed for \\$83 Million loss](#)
[George C. Kaplan](#)
- [Greenwich Mean Time just changed by one hour](#)
[Scot E. Wilcoxon](#)
- [GPS glider pilot confused](#)
[Philip Overy](#)
- [Printing with different resolutions in MS Word 7.0](#)
[Thiemo Sammern](#)
- [Re: Crackers Obtained Gulf War Military Secrets](#)
[Gene Schultz](#)
- [Millennium Bug: latest sighting](#)
[Pete Mellor](#)
- [Re: More Y2K Cost Estimations](#)
[James Byers](#)
[Martin Minow](#)
- [Re: Risks Associated with the Year 2000 Problem](#)
[Jack K. Horner](#)
- [Y2K: the revenge of originality / reserved words in Cobol](#)

[Henry G. Baker](#)

● [Re: Retiring hardware after Y2K](#)

[Barry Brown](#)

● [Y2K risks and Cobol](#)

[Jason D Lampert](#)

● [The unique risks related to Y2K](#)

[Peter Wild](#)

● [Info on RISKS \(comp.risks\)](#)

⚡ END OF VOLUME 18

"Peter G. Neumann" <Neumann@CSL.sri.com>

Mon, 31 Mar 1997 8:31:17 PST

The end-volume issue ([RISKS-18.97](#)) is available on the ftp site as

[risks-18.00](#) in the main directory, and is now also in the new subdirectory

18 as both [risks-18.00](#) and [risks-18.97](#) -- along with the rest of volume 18.

⚡ Computer model blamed for \$83 Million loss

George C. Kaplan <gckaplan@cea.berkeley.edu>

Sat, 29 Mar 1997 17:25:35 -0800

The *Wall Street Journal*, 28 March 1997, reports that the derivatives trading unit of Bank of Tokyo-Mitsubishi Bank Ltd. has incurred an loss of \$83 Million as a result of a computer model that overvalued a portfolio.

The problem came to light last summer, when the model was revised. Another model-related loss, \$139 Million by National Westminster Bank

PLC is also mentioned.

The article points out the risks of increasingly complicated derivatives portfolios, which are so complex that traders have no choice but to use computer-based models to evaluate them.

But other sources point out that the real risks are the old familiar ones of trusting the computer too much. Thomas Coleman of TMG Financial Products Inc. says, "I've never seen an options model which, when used for the things it was meant to do by people who understood it, has caused a \$50 million to \$100 Million problem."

George C. Kaplan gckaplan@cea.berkeley.edu 510-643-5651

🔥 Greenwich Mean Time just changed by one hour

<sewilco@fieldday.mn.org>

Mon, 31 Mar 1997 08:44:14 -0600 (CST)

On my Linux machines, I keep the hardware clock on Universal time to avoid time-zone problems. One machine is used for both Linux and MS Win95, so I set the Win95 time zone to "Greenwich Mean Time". At least that's what the map on the Control Panel called it. I'm in the U.S.A. Central time zone, six time zones west of Greenwich.

This morning, Monday 31 March 1997, Win95 reported the time had been changed due to Daylight Savings Time. DST doesn't begin in the USA until next

Sunday, and I see that I had left the "Adjust for DST" checkbox set on the Win95 Control Panel. I then checked and apparently British Summer Time did indeed start yesterday in England.

<http://www.greenwich2000.com/timefaqg.htm>

But Win95 still labels that time zone as GMT, not BST. If you're trying to use Universal time on Win95, check your clocks today.

[http typo fixed in archive copy. PGN]

✈ GPS glider pilot confused

Philip Overy <pjo33@mailbox.rl.ac.uk>

Thu, 27 Mar 1997 14:25:15 +0000

Well, our club has now met its first lost pilot who was flying on GPS "lead and follow" when his box went wrong: At our airfield, GPS needs a "watch out for parachutists" function too; Although one might argue that this is not a risk of having the navigational aid, but of using it to the exclusion of all else, the truth is that at our sort of height none of the navigation methods are perfect - maps plus turning points are not that easy to cope with - so the lure of GPS will be hard to resist. When height-capable GPS-based devices begin to drive map displays and provide warnings, there will be real problems if such laptop or instrument-panel-mounted "aids" ever fail. I'm sure gliding clubs will make rules regarding GPS, however will the GPS device manufacturers consider the uses to which their products are being put?. When

you buy quack
medicines in a pharmacy, there is (in the UK at least...) a
warning to "consult
your doctor if symptoms get worse" - perhaps there should be a
warning on GPS
systems to learn navigation before you depend too much on this
aid?.

Phil Overy Computer security officer RAL, CLRC, UK tel (44) (0)
1235 (44) 5834

🔥 Printing with different resolutions in MS Word 7.0

Thiemo Sammern <tsamm@ping.at>
Sun, 30 Mar 1997 14:06:44 +0100

This story could be interesting for comp.risks-readers. Please
note, that
it isn't a Y2K-problem :-)

I recently installed a new HP LaserJet printer in my father's
law office.

As most new laser printers it is capable of printing with a
600dpi

resolution. One of our secretaries has her own printer
connected to her

workstation. This printer is an older LaserJet model and has
only 300 dpi

resolution. Sometimes she prints on her small printer and
sometimes

(especially longer and double- sided documents) on the new
printer. We use

Win95 and Word 7.0. After about a week she told me, that the
printout

sometimes differs a lot between the two printers. It happens
quite often

that some lines in our documents contain only a few words and
the rest of

the line is filled with dots or dashes. She knows about the
possibility to

set tabs with filling characters but doesn't want to use it. So she makes loads of dots and dashes in these lines manually. It happened, that these lines were printed different on the two printers. The printout on her small printer was always correct, but when she switched to the other printer the last dot or dash of the line jumped to the next line and so sometimes changed the whole page.

I found out, that this behaviour didn't occur when I set the new printer back to 300dpi resolution (the same resolution the old printer has). I think the problem lies in the "GetTextWidth"-function in the Windows API or the way Microsoft Word uses it. This function returns the number of dots a character (or textstring) needs as an integer value and therefore is only a coarse approximation of the correct value. If the function is called for each character in the line separately a possible rounding error gets multiplied. And I think this happened in our case. Word calculated different textlengths for the same text on different printers.

The risks? Sometimes single pages of the documents are printed selectively because of typos or new data. The above mentioned error could have lead to a change in the page layout, maybe moving important parts of the document to another page not included in the new printout. I don't want to imagine the effects :-)

I hope this message lets some people take a closer look at their printed documents.

Thiemo Sammern, St. Lorenz 444, 5310 Mondsee, Austria-Europe
+43/6232/54006 tsamm@ping.at <http://members.ping.at/tsamm>

✦ Re: Crackers Obtained Gulf War Military Secrets ([RISKS-18.94,95](#))

Gene Schultz <gschultz@isl.sri.com>

Mon, 31 Mar 1997 09:07:00 -0800

The recent set of news articles and net postings are the result of an interview with BBC late in January 1997 in London. BBC was trying to do a story on breakins into banks in London. They persuaded me to supplement the content with an example of what could happen if security is lax in another arena---the military. I shared with the interviewer, Riccardo Pollack, an account of breakins into U.S. military computers during Operation Desert Shield/Desert Storm. What I told him was that I headed the U.S. Department of Energy's Computer Incident Advisory Capability (CIAC) (which I founded and kept going for 3.5 years despite working in an extremely adverse political and managerial environment that ultimately caused the entire team with the exception of one part-time person to quit). The AP news story that followed somehow distorted this by claiming that I was the head of computer security for the Department of Energy. Actually, I had responsibility for running the CIAC team and for developing the team's procedures and operations was clearly mine -- as the project manager.

Second, the AP news story quotes me as saying that top-secret information was stolen. This assertion is totally inaccurate. I would say, however, that a considerable amount of information that was not designated with any sensitivity labels was stolen from U.S. military computers. The fact that so much sensitive/critical information was stored on computers that were so easy to reach and break into is beyond all comprehension. What was perhaps worse, however, was that the U.S. Government didn't really deal with the incidents very well at all. Turf wars between agencies (as well as within LLNL) were a constant problem, for example, and nobody within the Government really seemed to have jurisdiction over the case. One of the main FBI players at one point told all other incident-response teams who were producing information about the attacks to "butt out" because he wanted to work only with the one particular response team he favored. One of the Government agencies ordered that a computer that was being used very productively to monitor the intruders be shut down to avoid further trouble, even though the compromised computer was not a sensitive one. In short, the whole situation was a real "three-ring circus." Some day I hope to document the whole fiasco. Meanwhile, I have already provided a lot of details in my Congressional testimony in November 1991 and also in a paper published in the Proceedings of the 1993 Department of Energy Computer Security Group Workshop.

I'd like to help more by providing more information, but I'm off on a three-week consulting stint overseas. Again, I'd encourage those who have so greatly contributed to the confusion surrounding the BBC documentary to simply purchase the tape (videotapes are now publically available) and find out what was really said.

Gene Schultz, Program Manager, SRI Consulting

✶ Millennium Bug: latest sighting

Pete Mellor <pm@csr.city.ac.uk>

Fri, 28 Mar 1997 11:48:24 GMT

My friend and colleague Norman Fenton <nf@csr.city.ac.uk> seems to attract the Millennium bug. Instances of it follow him around like storm clouds following a rain god.

Here is his report of his latest sighting:-

I actually witnessed a millennium bug in action last week at a hotel. The receptionist was trying to enter a renewed membership (which had arrived by post) for the health club on the computer system. The member in question had paid for a 3-year membership which was therefore to expire in March 2000. The system used 2-digit years. The year 00 was rejected (it was clearly treating it as 1900 because it came up with an error message something like 'date expired').

The receptionist in the end decided to enter the date 31Mar99 as

the expiry
date. Hence this unsuspecting member is being cheated out of 3
months
membership. I wonder how many similar transactions are taking
place all
over the world at this moment.

Norman

[Note added in archive copy: Well, you get the idea.
That must be either 31Dec99 or 9 months. PGN]

✂ Re: More Y2K Cost Estimations (Schroeppel, [RISKS-18.95](#))

James Byers <jwb19@cornell.edu>
Sat, 29 Mar 1997 05:25:53 -0500

I encourage anyone interested in a "serious discussion" of Y2K
costs to read
Capers Jones' article "THE GLOBAL ECONOMIC IMPACT OF THE YEAR
2000 SOFTWARE
PROBLEM" in full (<http://www.spr.com/library/y2k00.htm>).

Indeed, Jones
estimates the long term global economic impact of Y2K fixes,
downtime,
litigation, etc. at \$1.6E12. Sound excessive? Perhaps, but
Jones presents
a substantial case based on function point metrics rather than
"lines of
code" metrics used in analyses by the Gartner Group and others.

A disturbing feature of Jones' analysis is his casual and
frequent
disclaimer about the potential for inaccuracy in many of his
assumptions.
He notes that his charts are "rough approximations" and have a
"high margin
of error." Skeptics such as myself do not swallow these
statements easily.

While Jones presents a substantial body of evidence, more rigorous surveys of real data on the Y2K dilemma are sorely needed. Yet time again seems to be against us, as surveys with the depth and breadth of information needed for better Y2K cost approximations would likely not be completed nearly in time to be beneficial.

We can only hope that Jones grossly overestimates the cost of this whole affair. One thing is certain, however: the more informed believers and skeptics alike can be on the issues surrounding Y2K, the better. Blind judgements on the issue will only increase the potential for a catastrophe on 1/1/2000 and beyond.

James Byers - byers@cornell.edu - <http://www.people.cornell.edu/pages/jwb19>

✉ Re: More Y2K Cost Estimations ([RISKS-18.94,95](#))

Martin Minow <minow@apple.com>

Fri, 28 Mar 1997 14:01:49 -0800

My RISKS article might have been clearer in noting that the total cost refers to the total global cost, not just the cost in Sweden (see below) I skimmed the report (and recommend it highly). Jones estimates the total cost for U.S. software at 70.8 billion dollars (with a "large, but unknown margin of error").

Capers Jones also describes loss of data center productivity,

estimated as
10% (best-case), 25% or higher (most probable), to 35% (worst
case).

"Although this data has a high margin of error, it appears that
the repair
costs for the year 2000 problem may be one of the largest single
technology
expenses in human history."

Jones' article concludes with estimates for thirty countries.
Sweden is at
the bottom of the list, with an estimate of 267,188 effort-
months, or 2.87%
of the American effort. (Again, with warnings for incorrect
assumptions.)

Swedish burdened salary costs are almost 10% higher than America
[I ought to
move back] and the Swedish total cost is estimated at \$2.4
billion, with the
total for all countries estimated at almost \$300 billion.

The Swedish text may (repeat, may) be in error regarding the per-
capita
cost. Capers Jones gives the following estimate for Sweden:

Burdened Salary:	\$9,200 / month
Total effort months:	267,188
Total repair costs	\$2,458,125,000

Estimating 8.5 million citizens, this yields \$289 dollars/person
for Swedish
costs. However, Freese estimates 240 billion SKR, roughly \$34
billion, or
\$4000 / citizen. I don't know why Freese's cost estimate is
about 6 times
higher than Jones, but suspect that they're measuring different
things.

Capers Jones is the author of Applied Software Measurement
(McGraw Hill,
1996). What little I've seen of his work, appears to be serious
and well

thought out, if perhaps a bit over-precise for my tastes.

Martin

[Also comments on Capers Jones from Rob Bailey <wm8s@pobox.com>. PGN]

✦ Re: Risks Associated with the Year 2000 Problem

"Jack K. Horner 120775" <jkh@lanl.gov>

Thu, 27 Mar 1997 11:10:33 -0700

[This is message sent to Rick Light <rxl@LANL.GOV> in response to a forwarding of a comment on the appended message from the U.S. House Science Committee, particularly relating to those Y2K

problems resulting from the omission of the "19" in the calendar

year. It is reproduced with the permission of the author. PGN]

The problem is potentially much messier than just the occurrences of the literal value "19" in date types. ANYTHING in software that merely _acts as if_ the first two digits of the date are "19" will have insidious effects.

About a year ago, I worked on an analysis of the Global Positioning System (GPS) ground station code to try to characterize the Y2K problem. We found no less than ten types of manifestations of the problem in a survey of a randomly selected sample of 10% of the code. The occurrence of the literal value "19" was only one of these ten types. Other types included type overflow problems at various dates throughout 1999, Y2K arithmetic that implicitly assumed no

dates later than 31 Dec 99 were possible, and implicit module-interface date-type conversions. These problems are potentially infinite in their variety, and not all can be detected with tools. Furthermore, in GPS it is not possible to construct good test cases to see what will happen at the millennium start, because the future (time-) states of the system depend on physical values (orbital elements, pole wander, Jovian gravitational force) that can be determined with sufficient accuracy only from the actual operation of the system within about three months of the time of interest. Approximately 1% of the total GPS code is affected by this class of problems, or affected it.

The GPS user-equipment code is in even deeper trouble because of the Y2K problem, and the breakage will occur well before Jan 1, 2000. Date, in the GPS signal standard, uses exactly thirteen bits (these bits represent a time-unit offset from a conventional epoch date). This allocation is burned into proms on all existing GPS user equipment. On about August 20, 1999, the actual date value will overflow this 13-bit type, and the equipment will fail to produce correct time or position information. Best estimate is that there are $\sim 10^6$ pieces of user equipment that will be immediately affected. Everybody who depends indirectly on those pieces of equipment (meaning all the rest of us) will also be affected. The GPS standards committee is desperately trying to figure out what to do with the problem.

Various well-calibrated software estimation models (SLAM, REVIC, PRICE-S)

predict that fixing the Y2K problem in systems of about 500,000 lines of code or larger will take more time than is available between now and the year 2000, regardless of how many programmers are thrown at the job. Most of the US's military command-and-control systems contain more than 500,000 lines of code.

GPS is now the primary means of distributing time standards throughout the US, and throughout much of the world. (The accuracy of the atomic clocks on board the GPS satellites is second only to those maintained by the primary standards clocks in Washington.) Thousands of large financial computers ultimately take their time calibration from GPS, every day. Interest on overnight multi-billion-dollar short-term electronic-funds transactions is computed at millisecond granularity, derived from the GPS standard.

Place your bets.

Jack Horner, CIC-8

>>Notice From:
>>United States House of Representatives
>>Committee on Science
>>F. James Sensenbrenner, Jr., Chairman
>>George E. Brown, Jr., California, Ranking Democrat
>
>>CONSUMER RISKS ASSOCIATED WITH YEAR 2000 PROBLEM CITED
>>
>>Washington, DC -- Rep. Constance A. Morella, chair of the Committee on
>>Science's Subcommittee on Technology, along with several of her
>>colleagues sent a letter today to the Clinton Administration requesting
>>information on the Year 2000 problem.

>>
>>"We initially thought the problem affected just computer software and
>>programs, but we are now learning that the magnitude and scope of the
>>Year 2000 challenge seems to be growing beyond just computers," Morella
>>stated. "If consumer products which contain microchips are affected, we
>>need to know whether agencies are addressing this fact and whether the
>>American public is being adequately informed."
>>
>>The Year 2000 problem involves embedded microchips which are present in
>>many every day conveniences such as microwaves and elevators. Most of
>>these products have internal timers which are programmed with the "19"
>>prefix. When the year 2000 is ushered in, computers which are
>>programmed with the "19" prefix will interpret the year to be 1900 -
>>not year 2000. Some experts are predicting that if corrective actions
>>are not taken by the year 2000, businesses and possibly some sectors of
>>the government could face operational and fiscal disasters.
>>
>>"The Year 2000 problem poses a daunting challenge to consumers,
>>businesses, and government alike," said Representative Bart Gordon,
>>ranking Democrat on the Subcommittee who also signed the letter. "I
>>look forward to working with Chairwoman Morella to increase the public's
>>awareness of the potentially catastrophic consequences if the Year 2000
>>problem is not addressed."
>>
>>The letter was drafted after a hearing last week in which several
>>witnesses reiterated their concerns about potential serious safety

>>consequences associated with the Year 2000 problem. One study discussed
>>predicted that more than one-half of all organizations world-wide will
>>not fully complete the Year 2000 effort.
>>
>>"If the long-term forecast for the Year 2000 problem is dismal, there
>>must be a realization of failure, and new strategies must emerge from
>>this realization," Morella said. She also said the response to the
>>inquiry would assist her Subcommittee with identifying Year 2000
>>situations which may affect the health and safety consequences of
>>consumers.
>>
>>In addition to Morella and Gordon, the letter was also signed by
>>Representative Stephen Horn, chair of the Government Reform and
>>Oversight Committee's Subcommittee on Government Management,
>>Information, and Technology and Representative Carolyn Maloney, ranking
>>Member on the Subcommittee on Government Management,
>>Information and
>>Technology.

✶ Y2K: the revenge of originality / reserved words in Cobol

Henry G. Baker <hbaker@netcom.com>
Mon, 17 Mar 1997 14:02:43 -0800 (PST)

Re: programmers who use random words for identifiers in Cobol:

I have argued [1] against certain features of programming languages that 'blow up' the number of identifiers that a programmer has to come up with. Interestingly, although do-while loops save labels,

Dijkstra

[2] leaves it up to Wirth & Hoare to make this point with regard to the 'case'/'switch' construction: "...it eliminates the need for introducing a large number of labels in the program".

A previous posting mentioned that Cobol has something like 300 reserved words. I have argued [3] that languages not use real words

for their reserved words, because

- * unreal words are much easier to spot by both experienced and non-experienced

 - programmers;

- * every programmer must learn the reserved words anyway, and using

 - real words like 'begin' or 'loop' wastes our visual bandwidth, and

 - seduces non-technical types into thinking that they can 'understand'

 - the program--a very dangerous situation;

- * by using real words as reserved words, some of the best and most

 - mnemonic words have already been stolen by the language.

Of course, PL/I's 'cure' is far worse than the disease; parsing PL/I's

'nonreserved' reserved words is a nightmare for both computers and people.

1. Baker, H.G. "A Source of Redundant Identifiers in PASCAL Programs". ACM Sigplan Notices 15, 2 (Feb. 1980), 14-16.

Available

on my web page.

2. Dijkstra, E.W. "Goto To Statement Considered Harmful". CACM 11,3

(March 1968), 147-148, reprinted in CACM Oct. 1995. Available on www.acm.org.

3. Baker, H.G. "Strategies for the Lossless Encoding of Strings as

Ada Identifiers". ACM Ada Letters XIII,5 (Sep/Oct 1993), 43-47. Available

on my web page.

Henry Baker <ftp://ftp.netcom.com/pub/hb/hbaker/home.html>

✶ Re: Retiring hardware after Y2K

Barry Brown <bbrown@dottie.sna.com>

Mon, 24 Mar 1997 16:39:01 -0800 (PST)

To what extreme do we have to take this? The world is spending money now to update all of the computers to four-digit years. Who's to say we won't have to do this all over again with our 8000-year-old programs when the year 10,000 approaches? Are we being shortsighted by not implementing five- or six- or more-digit dates right now?

Barry

✶ Y2K risks and Cobol

"LAMPERT, JASON D" <jdlamp@GNV.IFAS.UFL.EDU>

Fri, 28 Mar 1997 09:51:40 -0500 (EST)

The following is taken from Monday March 24, 1997 edition of the *Gainesville Sun* in the Worklife Section:

A renewed use for COBOL

Cobol, a programming language created in the '50s and in decline through

most of the '80s is in the midst of a revival. Cobol is the language that

enables old mainframe computers to correctly handle dates

after the year

2000 [!!!]. Consultants SPR Inc. in Oakbrook, Ill has trained over 65

nonprogrammers in it in the past year, with 15 more now enrolled in the

two-month Cobol "Boot Camp."

[Corporation X] drills "newbie" programmers in a one month course. At

Columbus State Community College in Ohio, Cobol enrollment has jumped by

a third. Even a home-study course has emerged, promising Cobol proficiency in three weeks.

Going beyond the error in fact about Cobol in the above article, okay, so we

have the Y2K problem, which involves scanning millions of lines of code, and

rewriting thousands of them, then debugging the new code, then testing it.

And to this very complex and difficult project we're going to assign someone

with a 3 week home study course in cobol. Not just a little risky.

Jason Lampert, Computer Support Specialist, UF Dept of Plant Pathology

Jdlamp@gnv.ifas.ufl.edu

⚡ The unique risks related to the Year 2000

Peter Wild <peter.wild@worldnet.att.net>

Mon, 31 Mar 1997 02:11:50 +0000

These are some of the RISKS associated with the first real Information

Technology {IT} project that demands fixed functionality to be delivered on

a fixed date.

1. Many installations do not contract for their development & testing capacity to be included in their Disaster Recovery Contracts with organizations such as Comdisco, Sunguard and IBM. This must be done now because, in the event of an outage, there will be an increasing need to test & develop Y2K solutions.

2. The cost of all resources will increase and they will become more scarce as more are drawn towards the Y2K work which will increasingly pay more. We are already seeing consulting staff leaving engagements (which are not Y2K related) because they have been hired away by other firms. Also rates are beginning to increase. Even mainframe tape cartridges are beginning to become more scarce the same will happen to other commodities such as DASD, computers etc. It will also become increasingly more serious as people begin to place larger, speculative orders to protect themselves - the siege mentality.

3. There are attorneys who, today, are employing people to cut out every reference any company official is making in the press about their corporate Y2K process and readiness ... so they can be quoted if there is a law suit because they failed.

[...]

peter.wild@worldnet.att.net



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